

JC930 U.S. PTO
00/8T/60

Please type a plus sign (+) inside this box →

09-19-00 A

PTO/SB/05 (4/98)

Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No. **N0064 US**

First Inventor or Application Identifier **CHQJNACKI**

Title **Method + System for Mass Distribution of Geographic Data for Navigation Systems**

Express Mail Label No. **EK 656528364 US**

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

- * Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
- Specification [Total Pages **61**]
(preferred arrangement set forth below)
 - Descriptive title of the Invention
 - Cross References to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference to Microfiche Appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
- Drawing(s) (35 U.S.C. 113) [Total Sheets **13**]
- Oath or Declaration [Total Pages **2**]
 - a. Newly executed (original or copy)
 - b. Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 16 completed)
 - i. DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

*NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.37), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

Assistant Commissioner for Patents
ADDRESS TO: Box Patent Application
Washington, DC 20231

5. Microfiche Computer Program (Appendix)
6. Nucleotide and/or Amino Acid Sequence Submission
(If applicable, all necessary)
 - a. Computer Readable Copy
 - b. Paper Copy (identical to computer copy)
 - c. Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. Assignment Papers (cover sheet & document(s))
8. 37 C.F.R. § 3.73(b) Statement Power of
(when there is an assignee) Attorney
9. English Translation Document (if applicable)
10. Information Disclosure Statement (IDS)/PTO-1449 Copies of IDS
Citations
11. Preliminary Amendment
12. Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
 - * Small Entity Statement filed in prior application,
Statement(s) Status still proper and desired
(PTO/SB/09-12)
 - 13. Certified Copy of Priority Document(s)
(if foreign priority is claimed)
 - 14. Other:
.....

16. If a CONTINUATING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

Continuation Divisional Continuation-in-part (CIP) of prior application No: _____

Prior application information: Examiner _____ Group / Art Unit: _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

Customer Number or Bar Code Label (Insert Customer No. or Attach bar code label here) or Correspondence address below

Name	Frank J. Kozak, Esq.		
	Navigation Technologies Corporation		
Address	10400 West Higgins Road		
City	Rosemont	State	IL
Country	USA	Telephone	847/795-7371
Zip Code	60018		
Fax	847/699-8057		

Name (Print/Type)	Frank J. Kozak	Registration No. (Attorney/Agent)	32,908
Signature		Date	

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL

for FY 2000

Patent fees are subject to annual revision.

Small Entity payments must be supported by a small entity statement, otherwise large entity fees must be paid. See Forms PTO/SB/09-12. See 37 C.F.R. §§ 1.27 and 1.28.

TOTAL AMOUNT OF PAYMENT (\$ 1150.00)

Complete if Known

Application Number	SEPT. 18, 2000
Filing Date	CHOZNACKI
First Named Inventor	
Examiner Name	
Group / Art Unit	
Attorney Docket No.	Noob64 US

METHOD OF PAYMENT (check one)

1. The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number 50 0728

Deposit Account Name Navigation Technologies

Charge Any Additional Fee Required Under 37 CFR §§ 1.16 and 1.17

2. Payment Enclosed:
 Check Money Order Other

FEE CALCULATION (continued)**3. ADDITIONAL FEES**

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
105	130	Surcharge - late filing fee or oath	
127	50	Surcharge - late provisional filing fee or cover sheet.	
139	130	Non-English specification	
147	2,520	For filing a request for reexamination	
112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	Requesting publication of SIR after Examiner action	
115	110	Extension for reply within first month	
116	380	Extension for reply within second month	
117	870	Extension for reply within third month	
118	1,360	Extension for reply within fourth month	
128	1,850	Extension for reply within fifth month	
119	300	Notice of Appeal	
120	300	Filing a brief in support of an appeal	
121	260	Request for oral hearing	
138	1,510	Petition to institute a public use proceeding	
140	110	Petition to revive - unavoidable	
141	1,210	Petition to revive - unintentional	
142	1,210	Utility issue fee (or reissue)	
143	430	Design issue fee	
144	580	Plant issue fee	
122	130	Petitions to the Commissioner	
123	50	Petitions related to provisional applications	
126	240	Submission of Information Disclosure Stmt	
581	40	Recording each patent assignment per property (times number of properties)	40
146	690	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	690	For each additional invention to be examined (37 CFR § 1.129(b))	
Other fee (specify) _____			
Other fee (specify) _____			
SUBTOTAL (3) (\$ 40.00)			

* Reduced by Basic Filing Fee Paid

SUBMITTED BY

Name (Print/Type)	Frank J. Kozak	Registration No. (Attorney/Agent)	32,908	Telephone	847/795-7371
Signature	<i>Frank J. Kozak</i>				Date Sept. 18, 2000

WARNING:

Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

PATENT
Atty. Docket. N0064US

**APPLICATION FOR A UNITED STATES PATENT
UNITED STATES PATENT AND TRADEMARK OFFICE**

INVENTOR: ROBERT CHOJNACKI

TITLE: METHOD AND SYSTEM FOR MASS
DISTRIBUTION OF
GEOGRAPHIC DATA FOR
NAVIGATION SYSTEMS

ATTORNEYS: Frank J. Kozak
Lawrence M. Kaplan
NAVIGATION TECHNOLOGIES
CORPORATION
Rosemont, Illinois 60018
(847) 795-7000

002760-7629-0000

1 METHOD AND SYSTEM FOR MASS DISTRIBUTION OF
2 GEOGRAPHIC DATA FOR NAVIGATION SYSTEMS

3 INCORPORATION BY REFERENCE

4 This specification is filed contemporaneously with two other U.S. patent applications,
5 entitled respectively "Encryption Method for Distribution of Data" and "Navigation System with
6 Decryption Functions and Secure Geographic Database," each by the same inventor as the present
7 invention, and each assigned to the owner of the present invention. The entirety of each of these
8 other applications is hereby incorporated by reference.

9 This specification is also related to the subject matter of U.S. Patent No. 5,951,620 (the
10 '620 patent), which is entitled "System and Method for Distributing Information for Storage
11 Media," and which issued on September 14, 1999 to Navigation Technologies Corporation of
12 Rosemont, Illinois. The entirety of the '620 patent is also hereby incorporated by reference.

13

14 BACKGROUND OF THE INVENTION

15 **1. Field of the Invention**

16 The present invention relates to a system and method for secure distribution of digital
17 data to end users' media for use by the end users. More particularly, the present invention relates
18 to systems and methods for distributing geographic data to end users for use in their navigation
19 systems.

20 **2. Description of Related Art**

21 There are various different types of devices for which end users are required to obtain
22 digital data. One type of device for which end users are required to obtain digital data is a
23 navigation system. Navigation systems for use on land have become available in a variety of

1 forms and provide for a variety of useful features. One exemplary type of navigation system
2 uses (1) a geographic database that contains data representing features in a geographic area or
3 region, (2) a navigation application program, (3) appropriate computer hardware, such as a
4 microprocessor and memory, and, optionally, (4) a positioning system. The geographic database
5 portion of the navigation system includes information about the positions of roads and
6 intersections in or related to a specific geographic regional area, and may also include
7 information about attributes, such as one-way streets and turn restrictions, as well as about street
8 addresses, alternative routes, hotels, restaurants, museums, stadiums, offices, automobile
9 dealerships, auto repair shops, etc.

10 The positioning system may employ any of several well-known technologies to
11 determine or approximate one's physical location in a geographic regional area. For example, the
12 positioning system may employ a GPS-type system (global positioning system), a "dead
13 reckoning"-type system, or combinations of these, or other systems, all of which are well-known
14 in the art.

15 The navigation application program portion of the navigation system is typically a
16 software program that uses data from the geographic database and the positioning system (when
17 employed). The navigation application program may provide the user with a graphical display
18 (e.g. a "map") of his specific location in the geographic area. In addition, the navigation
19 application program may also provide the user with specific directions to locations in the
20 geographic area from wherever he is located.

21 The geographic data used by a navigation system may be stored locally with the
22 navigation system in the vehicle, or, alternatively, the geographic data may be located remotely
23 and downloaded to the navigation application programs, as needed, via a wireless

1 communications system or other suitable communications channel. An advantage associated
2 with having the geographic data stored locally with the navigation system is that a large amount
3 of data is continuously available to the navigation system, thereby avoiding the costs associated
4 with installing and maintaining a communications infrastructure that affords the necessary
5 bandwidth needed to provide the data from a remote site. On the other hand, a consideration
6 associated with storing geographic data locally with the navigation system is the need to update
7 the data on a regular basis.

8 Accordingly, there is a need for a system and method for the distribution of new and
9 updated geographic data to users of navigation systems.

10 Another consideration associated with providing geographic data for navigation systems
11 is the need to safeguard the data from unlicensed uses, e.g., illegal copying. The collection of
12 geographic data can be a relatively time-consuming and expensive process. Therefore, although
13 it is desirable to make it easy for users of navigation systems to obtain new and updated
14 geographic data, it is also desired to provide security measures that prevent unlicensed uses.

15 As mentioned above, there are various different types of devices for which end users are
16 required to obtain digital data. Other devices include music players (e.g., audio CD players,
17 MP3 players, as well as players that support other formats), video game consoles, DVD players,
18 and computers. The considerations relating to safeguarding of geographic data from unlicensed
19 uses also applies to data provided for these other types of devices.

20

21 SUMMARY

22 The present invention provides a method and system for mass distribution of data. In
23 accordance with an exemplary embodiment of the invention, an authorization server may be

1 coupled via a communications link with a plurality of data distribution terminals. The
2 authorization server may maintain at least a first portion of each of a plurality of data products,
3 such as geographic databases for instance. The first portion may define parameters (such as
4 compression parameters and pointers) to which a machine must have access in order to be able to
5 usefully access the data product. Each data distribution terminal may, in turn, maintain the
6 remainder (i.e., a second portion) of each of a plurality of the data products. Thus, to establish a
7 complete data product, the authorization server may provide the first portion to a given data
8 distribution terminal, and the data distribution terminal may combine the portions together.

9 A person may visit one of the data distribution terminals to request a given data product
10 for use by a machine. The person may couple a portable data storage medium with the data
11 distribution terminal, and the user may provide the terminal with identification and payment
12 information. The terminal may then request the first portion of the data product from the
13 authorization server, the authorization server may verify authorization to provide the data
14 product, and the authorization server may then send the first portion to the terminal. The
15 terminal may then combine the first and second portions together and write the combined data
16 product to the data storage medium. The person may then remove the storage medium from the
17 terminal and couple the storage device with the machine. The machine may then read the data
18 product from the storage medium and use the data product.

19 This arrangement is well suited for supplying data products of various sorts for use by
20 machines of various sorts. In an exemplary embodiment, the data products may be geographic
21 databases, for use by navigation systems (such as in-vehicle navigation systems, handheld
22 (portable) navigation systems, or general purpose computing devices equipped with navigation
23 system functionality, for instance). As other examples, the data products may be digitized songs

1 or videos (e.g., movies) for use by music or video players, or games for use by video game
2 consoles. Other examples are possible as well.

3 To help further secure the communication of the data product, the authorization server
4 may also tie the first portion together with an authorization key, sending both the first portion
5 and the authorization key to the data distribution terminal. The data distribution terminal may
6 then record on the portable data storage medium both the first and second portions of the data
7 product and the authorization key. In turn, the machine that reads the storage medium may use
8 the authorization key to validate and/or facilitate its access to the data product.

9 This added security feature may take various forms. In one respect, for instance, the
10 authorization server may encrypt the first portion of the data product before sending it to the data
11 terminal. A machine authorized to access the data product may have access to a first decryption
12 key necessary for decryption of the first portion and may therefore decrypt the first portion so as
13 to gain access to the data product.

14 In another respect, the authorization server may establish an authorization key defining
15 verification information, such as an identification of the machine authorized to access the data
16 product and an identification of the data storage medium authorized to store a copy of the data
17 product. The authorization server may encrypt the authorization key so as to produce an
18 encrypted authorization key that can be decrypted using a second decryption key. The
19 authorization server may then send to the data distribution terminal (i) the encrypted
20 authorization key, and (ii) the encrypted first portion of the data product, and the data terminal
21 may record this information onto the storage medium, together with the second portion of the
22 data product.

1 In turn, a machine authorized to access the data product may use the second decryption
2 key to recover the authorization key, and may then use the verification information defined by
3 the authorization key to verify authorization to access the data product. If authorized, the
4 machine may then use the first decryption key to decrypt the first portion of the data product,
5 thereby gaining access to the full data product.

6 Further advantageously, the second decryption key can itself be derived as a function of
7 an environmental parameter (e.g., a system parameter) such as an ID of the machine authorized
8 to access the data product or an ID of the storage medium authorized to hold the data product.

9 With this arrangement, a machine seeking to access the data product should have the correct ID
10 and should obtain the correct ID from the storage medium, otherwise the machine may be unable
11 to establish the second decryption key and may therefore be precluded from accessing the data
12 product. Consequently, this arrangement helps prevent access to (and use of) the data product by
13 an unauthorized machine and further helps to prevent access to (and use of) the data product if
14 the data product is recorded on (e.g., has been copied to) an unauthorized storage medium.

15 In an alternative embodiment, the authorization server may provide some or all of a given
16 data product more directly to the machine authorized to access the data product. For instance,
17 the authorization server may send an encrypted authorization key and the encrypted first portion
18 of the data product to the machine via a wireless telecommunications network (such as a cellular
19 telephone system), for instance. The machine may acquire the other portion of the data product
20 in the same way or by other means. For example, a person may visit a data distribution terminal
21 to load a storage medium with the second portion of a selected data product, and the person may
22 then couple the storage medium with the machine. To facilitate access to the data product, the
23 machine may then request the authorization material (e.g., the encrypted authorization key and

1 encrypted first portion) from the authorization server, and the authorization server may provide
2 the requested material if the machine is authorized to receive it.

3 These and other objects and advantages of the present invention will become apparent to
4 those of ordinary skill in the art by reading the following detailed description, with appropriate
5 reference to the accompanying drawings.

6

7 BRIEF DESCRIPTION OF THE DRAWINGS

8 Preferred embodiments of the present invention are described herein with reference to the
9 drawings, in which:

10 Figure 1 is a block diagram illustrating a system arranged to facilitate mass distribution of
11 geographic data to one or more navigation systems in accordance with an exemplary
12 embodiment;

13 Figure 2 is a block diagram depicting an exemplary authorization server;

14 Figure 3 is a perspective view of an exemplary data storage device for holding secured
15 data;

16 Figure 4 is a block diagram depicting components of the data storage device of Figure 3;

17 Figure 5 is a block diagram of an exemplary data terminal;

18 Figure 6 is a database having a critical portion and a data portion;

19 Figure 7 is a block diagram of an exemplary navigation system;

20 Figure 8 is a flow chart depicting an exemplary process that may be performed in order to
21 provide a database of geographic data to portable data storage device;

1 Figure 9 is a flow chart depicting a set of functional blocks that may be involved in
2 securing and providing data to a navigation system in accordance with an exemplary
3 embodiment;

4 Figure 10 is a flow chart depicting a set of functional blocks that may be involved in
5 retrieval, decryption and validation of the data at the navigation system in accordance with an
6 exemplary embodiment;

7 Figure 11 is a flow chart illustrating a set of functional blocks that may be involved in an
8 enhanced process of securing, conveying and accessing data in accordance with an exemplary
9 embodiment;

E10 Figure 12 is a flow chart illustrating a set of functional blocks that may be involved in
E11 another enhanced process of securing, conveying and accessing data in accordance with an
E12 exemplary embodiment; and

F13 Figure 13 is a block diagram illustrating an alternative system arranged to facilitate mass
F14 distribution of geographic data to one or more navigation systems in accordance with an
F15 exemplary embodiment.

1 DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

2 A. Exemplary System Architecture

3 Referring to the drawings, Figure 1 is a block diagram illustrating an exemplary system
4 10 arranged to facilitate distribution of geographic data to one or more navigation systems 16.
5 System 10 includes an authorization server 12 arranged to be connected by a communications
6 link 18 to a plurality of data distribution terminals 20. Each data distribution terminal is then
7 arranged to provide data to a distribution medium 22, which is, in turn, arranged to provide the
8 data to a navigation system 16.

9 Communications link 18 can take any of a variety of forms and can include any number
B0 of intermediate entities arranged to convey data from one point to another. For example, link 18
B1 can include or take the form of a telecommunications network including wireless communication
B2 interfaces (e.g., satellite, radio frequency (RF) cellular, or other interfaces) and/or landline
F13 communication interfaces (e.g., the ISDN, cable, fiber, copper, or other interfaces). As a specific
B4 example, link 18 may comprise the public switched telephone network. As another specific
B15 example, link 18 may comprise the Internet, to which authorization server 12 and each data
B16 distribution terminal can be connected by a broadband (e.g., cable or DSL) connection,
B17 point-to-point connection, or other suitable link.

18 Distribution medium 22 may take various forms as well and may vary from terminal to
19 terminal and from navigation system to navigation system. For example, distribution medium 22
20 may comprise an RF communications link between a terminal 20 and a navigation system 16.
21 As another example, distribution medium 22 may comprise a wired communication link between
22 a terminal 20 and a navigation system 16.

1 In the exemplary embodiment, distribution medium 22 comprises a portable data storage
2 device, which can be selectively coupled to a distribution terminal 20 and to a navigation system
3 16. Thus, in operation, geographic data can be communicated from authorization server 12 over
4 link 18 to a data terminal 20. Data terminal 20 can then record data onto a portable data storage
5 device 22, which can then be physically carried to, or otherwise coupled with, a navigation
6 system 16. Navigation system 16 can then read the data from device 22 and use the data to
7 provide navigation services for a user.

8 This and other arrangements described herein are shown for purposes of illustration only,
9 and those skilled in the art will appreciate that other arrangements and other elements (e.g.,
10 machines, interfaces, functions, etc.) can be used instead, additional elements may be added, and
11 some elements may be omitted altogether. Further, those skilled in the art will appreciate that
12 many of the elements and interfaces described herein are functional entities that may be
13 implemented as discrete components or in conjunction with other components, in any suitable
14 combination and location.

15 It should also be understood that various functions described herein as being performed
16 by one or more entities may be carried out by one or more processors executing an appropriate
17 set of machine language instructions stored in memory. Provided with the present disclosure,
18 those skilled in the art can readily prepare and compile appropriate computer instructions to
19 perform such functions.

20 Referring now to Figure 2, an exemplary authorization server 12 is shown in greater
21 detail. Authorization server 12 may take the form of a general purpose computer programmed
22 with a set of machine language instructions to carry out the functions described below. As
23 shown in Figure 2, exemplary authorization server 12 may thus include a processor 26, a data

1 store 28, a memory 30 and a data interface unit 32. These components may be coupled together
2 by a system bus or other link to facilitate communication. And the components may take various
3 forms. By way of example, processor 26 may be an Intel Pentium III microprocessor, data store
4 28 may be a flash memory, ROM and/or magnetic or optical hard disk drive, memory 30 may be
5 volatile RAM (random access memory), and data interface unit 32 may comprise a transceiver,
6 modem, antenna and/or other arrangement suitable for communicating over link 18.

7 Although Figure 2 shows components of authorization server 12 within a single entity,
8 those skilled in the art will appreciate that various components could equally be provided as
9 separate entities. For example, all or part of data store 28 could be provided as a database server
10 with a separate processor that is accessible by processor 26 via a computer network or other link.

11 In an exemplary embodiment, data store 28 may hold three data components: (i)
12 geographic data 36, (ii) program logic 38, and (ii) authorization database 40. Geographic data 36
13 may comprise one or more databases or data files that define geographical data, such as road
14 geometry attributes and position information, and point-of-interest information. The road
15 geometry attribute and position information may include data about the positions (e.g., latitude
16 and longitude coordinates) of streets and intersections in or related to a specific geographical
17 area, information about one-way streets, street lights, stop signs, turn restrictions, street
18 addresses, speed limits, and the like. Point-of-interest information may include data about the
19 positions of airports, car rental agencies, service centers, restaurants, hotels, health clubs, and the
20 like. The geographical data may include other or different data as well.

21 Geographic data 36 may also include special databases of information. For example,
22 geographic data may include Fodor's® Restaurant Guide or other such information, which
23 authorization server 12 may provide together with a basic geographic database if desired.

1 Program logic 38 may comprise a number of machine language instructions that define
2 routines executable by processor 26. In operation, these instructions can be loaded from data
3 store 28 into memory 30 and then executed by processor 26 to carry out functions described
4 below, such as establishing authorization keys and encrypting authorization keys and geographic
5 data, for instance. Program logic 38 also includes an operating system (not shown), such as
6 Unix, Linux® or Microsoft Windows®, for instance.

7 Authorization database 40 may include information that identifies entities authorized to
8 access and/or possess geographic data. The entities may be, for instance, a user, a navigation
9 system and/or a data storage device (such as a flash memory card or other flash memory
10 medium, for example). Thus, for example, a given user profile record may be keyed to a user ID
11 code and may indicate that (i) the user is authorized to obtain geographic data for a particular
12 geographical area, (ii) a navigation system with a particular navigation system ID code is
13 authorized to access and use the geographic data, and (iii) a storage device with a particular
14 storage device ID code is authorized to hold the geographic data.

15 Authorization database 40 may also define algorithms and keys that authorization server
16 12 may use to encrypt and/or otherwise secure geographic data. The process or keys used to
17 encrypt or otherwise secure data may vary depending on the make and model of the navigation
18 system that is expected to access the data, or depending on other factors. For instance, each
19 model navigation system may have a predetermined decryption key that can be used to decrypt
20 data encrypted using a corresponding encryption key and/or corresponding encryption algorithm.
21 More specifically, each model navigation system may have its own private/public key pair.
22 Authorization database 40 may therefore indicate, for each model navigation system, the
23 encryption key and/or algorithm to be used for securing data that will be accessed by that model

1 navigation system. (Data could be encrypted using a private key and then decrypted by the
2 navigation system using the corresponding public key, or vice versa.)

3 In practice, the geographic data that is stored in data store 28 will be updated regularly,
4 through a time consuming and costly process of surveying roads and points of interest and
5 collecting and compiling data. Consequently, authorization server 12, and particularly data store
6 28, is preferably maintained in a physically secure location, so as to guard against theft or
7 misappropriation of the geographic data. Authorization server 12 may be owned and operated by
8 a geographic data supply company, such as Navigation Technologies Corporation, of Rosemont,
9 Illinois, which provides geographic data for use in mapping and navigation systems.

10 As indicated above, geographic data can be recorded on portable data storage device 22,
11 which can then conveniently be provided to a navigation system 16. The storage device is
12 preferably portable (e.g., small and lightweight enough to carry), secure, nonvolatile, readable
13 and re-writeable. Further, the storage device preferably has sufficient storage capacity to hold
14 geographic data for a typical geographical area (such as a city, state, region, or any other sized
15 area). Still further, to be robust, the storage device is preferably arranged to hold data in an
16 appropriate format, such as the SDAL™ format available from Navigation Technologies
17 Corporation or that is described in U.S. Patent Nos. 5,968,109, 5,974,419, and 5,953,722.
18 However, storage device 22 can take other forms as well.

19 In an exemplary embodiment, portable data storage device 22 takes the form of a flash
20 memory card or PC card (PCMCIA card) with housing dimensions, interface dimensions and
21 data storage capacity that conform with industry standards, recommendations or specifications.
22 For example, if the storage device is a flash memory card, the device may conform with size and
23 capacity parameters conforming with SD Memory Card Specifications (available from the

1 Secure Digital Card Association of Palo Alto, California), which is well known to those skilled
2 in the art. Such cards currently have dimensions of about 31 mm x 24 mm x 2.1 mm and have
3 storage capacity of 32 megabytes or 64 megabytes of data. As another example, if the storage
4 device is a PCMCIA hard disk card, the device preferably conforms with the PCMCIA standard
5 (such as the PCMCIA Type III standard), which is well known to those skilled in the art. Such
6 PCMCIA cards have dimensions of about 85 mm x 54 mm x 5 mm and are presently capable of
7 storing about 440 megabytes of data.

8 Figures 3 and 4 illustrate an exemplary portable data storage device 22 in the form of an
9 SD-Card (e.g., a "SanDisk Secure Digital Memory Card," which is a flash memory card
10 manufactured by SanDisk Corporation of Sunnyvale, California). Figure 3 shows the card in
11 perspective, and Figure 4 is a schematic block diagram illustrating functional blocks of the card.
12 As shown, exemplary device 22 includes an external housing 102, internal flash memory or other
13 such storage segment 104, and a 9-pin serial interface 106 or other interface on or otherwise
14 extending from the housing. Housing 102 is preferably about 31 millimeters long, 24
15 millimeters wide and 2.1 millimeters thick, but may be any other desired dimensions as well.
16 Exemplary flash memory 104 may be large enough to hold 64 megabytes of data, by way of
17 example, and is shown to include a set of data 108, such as geographic data and authorization
18 parameters. Serial interface 106 comprises a set of pins or other connectors that can preferably
19 be coupled with a corresponding entity to facilitate reading from, writing to and otherwise
20 controlling the flash memory.

21 As another example, the portable data storage device 22 could reside in (or could be) a
22 personal data assistant ("PDA"), portable telephone or other such device. Many PDAs exist
23 today and provide either substantial data storage capacity and/or the capability to add expansion

1 data storage. Many PDAs include infrared communication ports or other wireless
2 communication interfaces. In this regard, for instance, the Bluetooth™ specification for short
3 range wireless communications could be employed to enable another entity, such as navigation
4 system 16 for instance, to read from, write to, or otherwise communicate with the PDA.

5 Portable data storage device 22 preferably has a unique identification (ID) code such as a
6 serial number for instance. This storage device ID is preferably stored permanently in the
7 storage device. For example, the storage device ID could be burned into ROM (read-only-
8 memory) or other permanent storage portion of the device.

9 As indicated above, each intermediate data terminal 20 may be arranged to receive some
P0 or all of data 108 from authorization server 12 and to write data 108 onto the portable data
P1 storage device 22. Figure 5 is a schematic block diagram showing an exemplary data terminal
P2 20 in greater detail.

P3 Data terminal 20 can be a general purpose computer programmed with a set of machine
P4 language instructions to carry out various functions. By way of example, data terminal 20 can be
P5 a personal computer in a home or business and may be accessible by a limited set of users.
P6 Alternatively, for example, data terminal 20 can be situated in, or can define, a kiosk or other
P7 public display and may be accessible in general by any users.

P8 As illustrated in Figure 5, data terminal 20 may include a processor 42, a data store 44, a
P9 memory 46, a data interface unit 48, a storage device interface 50, and a display 52. These
P10 components can be coupled together by a system bus (not shown). Further, each of these
P11 components may take various forms. By way of example, processor 42 may be an Intel Pentium
P12 III processor, data store 44 may be a flash memory, ROM and/or magnetic or optical hard disk
P13 drive, memory 46 may be RAM, data interface unit 48 may comprise a modem, transceiver,

1 antenna and/or other entity suitable for communicating over link 18 (as shown in Figure 1),
2 interface 50 may be arranged as necessary to read and write data on portable data storage device
3 22, and display 52 may be a VGA monitor. Other examples are possible as well.

4 Similar to data interface unit 32 of the authorization server, the arrangement and
5 operation of interface 50 may depend on the arrangement and operation of portable data storage
6 device 22. For example, if device 22 is a flash memory card as illustrated in Figure 3, then
7 interface 50 might comprise a flash card socket and controller as described above. As another
8 example, if device 22 is a PDA with an infrared port, then interface 50 might comprise a
9 corresponding infrared port and controller arranged to communicate data via infrared signals. As
B10 still another example, if device 22 includes an RF wireless transceiver, such as a transceiver
B11 conforming to the Bluetooth™ specification, then interface 50 could similarly include a wireless
B12 transceiver arranged to communicate data via RF signals. Interface 50 could take still other
B13 forms as well.

B14 Data store 44 may hold two data components: (i) geographic data 54 and (ii) program
B15 logic 56. Geographic data 54 can take various forms. For example, geographic data 54 can
B16 comprise one or more databases of geographical data each corresponding, respectively, to one or
B17 more geographical areas or types of information. However, in an exemplary embodiment,
B18 geographic data 54 preferably contains only a portion of each database of geographic data that is,
B19 by itself, not usefully accessible by a navigation system.

20 In this regard, a database or other such data product can include a set of critical
21 information (critical data) that permits the entire data product to be used. The critical
22 information could take various forms. For instance, the critical information could include a
23 number of indexes, pointers or global parameters that enable a machine (such as a computer

1 processor) to access the data product. As an example, for instance, a database may define a
2 number of records or other parcels of information, and the critical information in the database
3 may define pointers to where in the database the records or other parcels begin. As another
4 example, the useful data in a database may be compressed or encrypted using various algorithms
5 and parameters, and the critical information may serve as a key to the data by specifying the
6 parameters or algorithms that a machine should use in order to decompress or decrypt the data.
7 As yet another example, a number of records in a database may include a code representative of
8 a useful data value, and the critical information in the database may define (or point to) the
9 corresponding data value. Without access to the critical information, a machine may therefore be
10 unable to access the useful data in the database.

11 The critical information in a database may be stored in one block in the database or may,
12 alternatively, be distributed throughout the database. As an example, the information may be
13 stored in a header or other block at the beginning of the database. As another example, the
14 information may comprise a number of indexes and other general parameters disposed at the
15 beginning of each of a number of parcels throughout the database. Typically, the critical
16 information will comprise a relatively small portion of the database.

17 To illustrate, Figure 6 depicts a database 58 that has a critical portion 60 and a data
18 portion 62. Although Figure 6 shows these portions as discrete blocks, the two may be
19 interspersed with each other or arranged differently in the actual database. In general, the critical
20 portion 60 contains some or all of the critical information that serves as a key to facilitate access
21 to data in the data portion 62.

22 In an exemplary embodiment, the geographic data 54 contained in the data store 44 of the
23 terminal 20 excludes some or all of the critical portion 60 of each database product. In one

1 embodiment, the geographic data 54 contained in the terminal 20 excludes an arbitrary-sized
2 portion of each database product. The excluded arbitrary-sized portion corresponds to some or
3 all the critical portion of each database product. In one embodiment, the arbitrary-sized portion
4 corresponds to the first two kilobytes of the database product. Alternatively, the first two
5 kilobytes might not correspond exactly to the critical information portion of a geographic
6 database product. For example, the first two kilobytes may not include all the critical
7 information of the database product or may include all the critical information as well as some of
8 the data portion of the database product. However, by excluding the first two kilobytes of each
9 database, enough of the critical portion is excluded so as to render the remainder unusable. In
10 alternative embodiments, the arbitrary-sized portion may correspond to sizes other than two
11 kilobytes or parts of the database product of than the first part.

12 The geographic data 54 stored at the terminal 20 may include just the remaining portions
13 of each database product with the arbitrary-sized portions excluded. Alternatively, the
14 geographic data 54 stored at the terminal 20 may include entire database products with the
15 portions corresponding to the arbitrary-sized excluded portions replaced with random or
16 otherwise useless data.

17 In turn, the geographic data 36 in the data store 28 of the authorization server 12
18 preferably includes at least the arbitrary-sized portions of each database that are not stored at the
19 terminals 22. In this regard, the geographic data 36 maintained by the authorization server may
20 comprise the entire databases of geographic information, and the authorization server may be
21 programmed to parse the arbitrary-sized portions from a given database for transmission to a
22 terminal 20 upon authorization. Alternatively, in an exemplary embodiment, the authorization

1 server may regularly maintain the critical portion of each database as a discrete data block ready
2 to send to a terminal upon authorization.

3 Advantageously, with this arrangement, a person or other entity with access to data stored
4 in terminal 20 can be prevented from using the databases without proper authorization, and
5 namely without access to the actual critical portions of the databases. At the same time,
6 however, terminal 20 can readily obtain the necessary critical information from authorization
7 server 12 when appropriate and can record both the critical portion 60 and the data portion 62 on
8 storage device 22 for use by navigation system 16.

9 Authorization server 12 may provide geographic data 54 via link 18 to each data terminal
10 20 periodically, upon request, or in response to other designated stimuli. Authorization server 12
11 may, for example, send geographic data 54 to data terminal 20 via link 18 in off-hours, such as
12 overnight for instance. This way, if link 18 has limited bandwidth (e.g., if link 18 is the public
13 switched telephone network, and authorization server 12 and terminal 20 communicate with each
14 other over link 18 via a 56 kbps modem connection, or if link 18 comprises a network such as the
15 Internet that tends to be congested during normal daytime hours, for instance), geographic data
16 54 can be conveyed with little if any concern.

17 Alternatively, geographic data 54 could be provided to data terminal 20 in some other
18 manner. For example, geographic data 54 could be loaded onto a CD ROM, which can be
19 physically sent to data terminal 20. A technician can then insert the CD ROM into a suitable CD
20 ROM drive in the data terminal or an arrangement could be in place to read the data from the CD
21 ROM into data store 44.

22 Program logic 56 may comprise a number of machine language instructions that define
23 routines executable by processor 42. In operation, these instructions can be loaded from data

1 store 44 into memory 46 and then executed by processor 42 to carry out various functions such
2 as interfacing with a user via display 52 and sending data to interface 50, to be written to
3 portable data storage device 22. Program logic 56 also includes an operating system (not
4 shown), such as Unix, Linux® or Microsoft Windows®, for instance.

5 Data terminal 20 preferably has a unique terminal ID. This ID could be a network
6 address of the terminal or could be a more permanent terminal identifier. In the exemplary
7 embodiment, the terminal ID could be stored permanently in ROM or in another suitable manner.

8 Referring now to Figure 7, an exemplary navigation system 16 is illustrated in greater
9 detail. Exemplary navigation system 16 could be an in-vehicle navigation system or could reside
10 in a handheld (i.e., portable) device or other entity, such as a cellular telephone, PDA, pager,
11 computer or dedicated mapping or positioning device, for instance. Other examples are possible
12 as well.

13 In an exemplary embodiment, navigation system 16 includes a processor 64, a data store
14 66, a memory 68, a data interface unit 70, a positioning system 72, a display 74, and a user input
15 mechanism 76. These components may be coupled together by a bus or other communications
16 path. And the components can take various forms. By way of example, processor 64 may be an
17 Intel Pentium III microprocessor, data store 66 may be a flash memory, ROM and/or magnetic or
18 optical hard disk drive, memory 68 may be volatile RAM, data interface unit 70 may be any
19 interface suitable for facilitating communications with distribution medium 22, display 74 may
20 be an LCD display and/or other means (audible or visual) for presentation, and user input
21 mechanism 76 may be a keyboard, control knob or microphone, for instance.

22 In the exemplary embodiment, positioning system 72 outputs information about the
23 position of the navigation system (e.g., the position of a vehicle in which the system is located,

1 or the position of a person carrying the system, for instance). This information may be in terms
2 of latitude and longitude, distance and heading, or other suitable parameters. Positioning system
3 72 may comprise a GPS receiver, the arrangement and operation of which are well known to
4 those skilled in the art. Alternatively, positioning system 72 can take other forms. Positioning
5 system 72 also preferably includes an antenna 78 or other such device for receiving GPS
6 positioning signals from satellites or for receiving position information from other types of
7 entities.

8 Data store 66 may hold navigation program logic 80, which may comprise a number of
9 machine language instructions that can be loaded into memory 68 and executed by processor 64
10 to perform various functions, such as decrypting and validating data, and providing navigation
11 services, for instance. Data store 66 also holds an operating system (not shown), such as Unix,
12 Linux[®] or Microsoft Windows CE[®], for instance, which can also be loaded into memory 68 and
13 executed by processor 64. Program logic also includes a data access library used to access data
14 libraries such as SDAL, as described for instance in U.S. Patent No. 6,047,280 (the '280 patent),
15 the entirety of which is hereby incorporated by reference.

16 Although not shown in Figure 7, data store 66 can also hold other information, such as
17 geographic data for instance. In that event, navigation system 16 could obtain geographic data
18 via data interface unit 70 and store the geographic data in data store 66 or memory 68. This
19 geographic data may, for instance, be the data portion 62 of one or more geographic databases,
20 as shown in Figure 6 and described above. With this arrangement, the navigation system would
21 not be able to usefully access the geographic data of a given database until the navigation system
22 obtains the critical portion 60 of the database as well. In the exemplary embodiment, however,

1 geographic data is primarily maintained on portable data storage device 22 and is read by
2 processor 64 into memory 68 from device 22.

3 In the exemplary embodiment, as noted above, data interface unit 70 serves to facilitate
4 communication with portable data storage device 22. Therefore, data interface unit 70 preferably
5 includes a port for communicating with storage device 22. Similar to the interface 32 of the
6 authorization server and interface 50 of terminal 20, the arrangement and operation of data
7 interface unit 70 may depend on the arrangement and operation of portable data storage device
8 22. Thus, data interface unit 70 might comprise a flash card socket, an infrared port, and/or an
9 RF transceiver, for example.

P10 Some or all of the components of navigation system 16 are preferably located in positions
P11 where they are readily accessible to a user for whom navigation services are to be provided. For
P12 example, if navigation system 16 is an in-vehicle navigation system, display 74 and user input
P13 mechanism 76 may be integrated in the vehicle dashboard for easy access by a driver, and the
P14 other components of the system can be hidden behind the dashboard or in another suitable
P15 location.

B16 Data interface unit 70 may also be provided in the vehicle dashboard or could be hidden
B17 from view, depending on how the data interface unit 70 is arranged to communicate data. For
B18 example, if data interface unit 70 is arranged to communicate with portable data storage device
B19 22 via an electrical connection, then data interface unit 70, or at least an electrical connection to
B20 the unit, will preferably be exposed to facilitate user access. For instance, data interface unit 70
B21 could be arranged as a socket or slot within the vehicle dashboard, into which a flash card could
B22 be inserted, similar to the socket described above. On the other hand, if data interface unit 70 is

1 arranged to communicate with portable data storage device 22 via a wireless link, for instance,
2 then unit 70 could be hidden from the user.

3 Similarly, if navigation system 16 is provided in a handheld device, such as a PDA, a
4 cellular telephone or a dedicated positioning device, for instance, some of the components can be
5 provided on the exterior surface of the device so as to facilitate user interaction, and other
6 components can be hidden within the device. For example, on a PDA, a touch-sensitive display
7 could serve as both display 74 and user input mechanism 76, and an expansion port or other link
8 (e.g., an infrared port or antenna) could serve as the data interface unit 70. Other components of
9 the navigation system can then be incorporated internally with the normal components of the

10 PDA.

11 In an exemplary embodiment, navigation system program logic 80 uses the output of
12 positioning system 72, in combination with geographic data 108 stored on the portable storage
13 device 22, to provide navigation services, features and information to a user of the navigation
14 system. Using output from the positioning system 72 and geographic data 108, program logic 80
15 preferably provides a map 82, a direction indicator (e.g., a turn arrow) and/or other information
16 on display 74. A map 82, for instance, may illustrate the location of the navigation system in a
17 given geographical area. Program logic 80 may provide information about what points of
18 interest are available, distances to various points of interest, directions (visual and/or audible) to
19 a desired destination, such as a street address or point of interest, and so forth. User input
20 mechanism 76, which may comprise a control knob, keyboard, or microphone, for instance,
21 allows a user to specify a desired destination, in response to which program logic may generate
22 and display directions to the destination.

1 Navigation system 16 will likely have a specific make (vendor) and model number.
2 Additionally, navigation system 16 preferably has a unique navigation system ID, such as a serial
3 number or other code. In addition to uniquely identifying the navigation system, the navigation
4 system ID may also be indicative of the navigation system make and model. In an exemplary
5 embodiment, the navigation system ID is stored permanently in the navigation system, such as in
6 ROM for instance.

7 Navigation systems as described above can be manufactured and assembled and then
8 sold, rented or otherwise distributed to consumers through any suitable distribution channels.
9 For example, in-vehicle navigation systems can be sold or rented by car dealerships as optional
10 or standard equipment in vehicles. As another example, retail stores may sell dedicated GPS-
11 based navigation devices to users. As still another example, vendors may sell or otherwise
12 provide software navigation systems that use geographic data to generate maps and directions,
13 even without including or using positioning systems. Such navigation applications can be
14 executed by a computer that has functional elements similar to those of navigation system 16, for
15 instance.

16 When a user obtains navigation system 16, the user may also obtain a navigation system
17 ID card, which identifies the navigation system by its model number and navigation system ID.
18 The information on the card may be machine readable, such as via a magnetic strip or RF tag for
19 instance. The user may also obtain a user ID card or other indication of a user ID, which
20 uniquely identifies the user. The user ID card may similarly indicate the user ID in machine
21 readable form.

1 **B. Exemplary Provisioning of Geographic Data**

2 In order for navigation system 16 to provide navigation services, it should have access to
3 a database or other set of geographic data. With the exemplary embodiment as described above,
4 a database of geographic data can be provided to navigation system 16 on portable data storage
5 device 22. Therefore, according to the exemplary embodiment, when a user first obtains
6 navigation system 16, the user preferably also obtains a portable storage device 22, suitable for
7 containing geographic data. The user may obtain the data storage device 22 from the same entity
8 that provided the user with the navigation system 16.

9 For instance, when a user obtains a car that has a navigation system installed as standard
10 equipment, the car may come with a portable data storage device 22 as well. As another
11 example, when a user buys a navigation system at a retail outlet, the system may also include a
12 portable data storage device 22. Alternatively, the user may purchase the portable data storage
13 device separately or obtain the device at some other time or in some other way.

14 When the user first obtains the portable data storage device 22, the storage device might
15 come pre-loaded with geographic data for a specific geographical area (such as a city, state or
16 other region, for instance). In that event, however, the user may at some point wish to update the
17 set of geographic data on device 22 so as to have the data reflect more current road conditions
18 and points-of-interest. Alternatively, the user may at some point wish to replace the geographic
19 data on the storage device with geographic data for a different geographical area. Still
20 alternatively, storage device 22 may not contain any geographic data to start. In that event, the
21 user may wish to load a set of geographic data onto the storage device to facilitate operation of
22 the user's navigation system in a given geographic area.

1 Various processes may be employed in order to load a geographic database onto portable
2 storage device 22. As indicated above, for example, authorization server 12 can send some or all
3 of the database to intermediate terminal 20, and terminal 20 can then record the database onto
4 storage device 22. Figure 8 is a flow chart depicting an exemplary process that may be
5 performed in order to provide a database of geographic data to portable data storage device 22 in
6 this way, and in turn to provide the data for use by a navigation system 16.

7 As shown in Figure 8, at block 150, a user first couples storage device 22 with the
8 interface 50 of terminal 20. For example, if storage device 22 is a flash card, the user may insert
9 the card into a corresponding flash card socket at terminal 20. At block 152, terminal 20 detects
10 the presence of storage device 22 and reads the storage device ID from the permanent storage
11 portion of storage device 22. In this example, terminal 20 may also attempt to read geographic
12 data from the storage device and determine that the storage device does not yet contain
13 geographic data.

14 At block 154, terminal 20 then preferably prompts the user to input the user's ID (and
15 perhaps a personal identification number (PIN)) and the navigation system ID in connection with
16 which the user will want to use the geographic data. At block 156, the user supplies this
17 information. As indicated above, the navigation system ID and user ID can be encoded in
18 machine readable form on one or more ID cards. Terminal 20 may include means for reading
19 those cards and obtaining the user and system IDs. Alternatively, for instance, the user could
20 type or otherwise enter the user ID and navigation system ID into the data terminal.

21 At block 158, terminal 20 may then prompt the user to select from a menu of
22 geographical regions for which geographic data can be loaded onto device 22. The menu may,
23 for instance, list all of the regions for which data store 44 of terminal 20 currently contains

1 geographic data. (As noted above, in an exemplary embodiment, data store 44 may contain
2 geographic data in the form of only the data portions 62 of various geographic databases. Each
3 data portion maintained by terminal 20 could be labeled or otherwise cross-referenced to
4 correspond with a particular geographical region.)

5 At block 160, the user may then select a desired region (or multiple regions). At block
6 162, terminal 20 may then responsively prompt the user to indicate whether the user wishes to (i)
7 purchase the data or (ii) rent the data for a certain period of time or for a certain number of uses.
8 At block 164, the user may respond by selecting either "purchase" or "rent" with specified time
9 or uses for instance.

10 At block 166, terminal 20 may also prompt the user to select from a number of special
11 geographic data options. These options may take various forms. For instance, an option might
12 be for the user to be able to access Fodor's® Restaurant Guide and/or special geographic areas on
13 navigation system 16. Each option might have a corresponding option number. And terminal 20
14 may also prompt the user to select a desired period of use or number of uses for a given option.
15 At block 168, the user may respond to the terminal by selecting one or more options and criteria
16 for use.

17 At block 170, terminal 20 may then prompt the user to supply payment information, such
18 as a credit or debit card number for instance. And at block 172, the user may provide the
19 requested payment information. In an exemplary embodiment, the dealer that sold the user the
20 navigation system 16 and/or the storage device 22 may have provided the user with a pre-
21 payment code, which the user may supply to terminal 20 to satisfy payment. The dealer could
22 then be ultimately accountable for the payment.

1 At block 174, terminal 20 then sends via link 18 to authorization server 12 a set of
2 information preferably including (i) the user ID, (ii) the storage device ID, (iii) the navigation
3 system ID, (iv) the selected geographic region (which might be the database name, for instance),
4 (v) rental time period or times of use, if applicable, (vi) options and periods or numbers of use of
5 options, (vii) the terminal ID, and (viii) the payment information. Authorization server 12, in
6 turn, receives this set of information.

7 At block 176, authorization server 12 queries its authorization database 40 to determine
8 whether the user is already authorized to receive the requested geographic data to be stored on
9 the specified storage device and accessed by the specified navigation system. This query may be
10 keyed to the user ID provided from terminal 20 for instance. This example will assume that a
11 user record does not yet exist in authorization database 40.

12 In addition, if the user has provided a PIN in connection with the user ID, the
13 authorization server may verify that the PIN is correct, by reference to a PIN table in the
14 authorization database 40. In the event the PIN is not correct, the authorization server may
15 return a signal to the data terminal, indicating that the session cannot continue absent a correct
16 PIN.

17 At block 178, finding no corresponding user record, authorization server 12 establishes a
18 user record indicating that, for the user having the user ID, the storage device having the storage
19 device ID is authorized to hold a particular database of geographic data, and the navigation
20 system having the navigation system ID is authorized to access the particular database of
21 geographic data. Further, to the extent the user elected to rent the data for only a specific time
22 period or for a number of uses, authorization server 12 may record in the user record an

1 expiration date or a count of number of allowed uses. At block 180, authorization server 12 may
2 then prepare and send data to terminal 20, to be written to storage device 22.

3 Authorization server 12 can send to terminal 20 the entire database of geographic data
4 corresponding to the region selected by the user. (This database may be referred to as the
5 "selected database.") However, in the exemplary embodiment, terminal 20 is assumed to already
6 have the data portion 62 of the database stored in its data store 44. Therefore, conveniently,
7 authorization server 12 will preferably send only the critical portion 60 of the database to
8 terminal 20. Advantageously, this will take far less time than it would take for the authorization
9 server to send the entire database to terminal 20.

10 When the critical portion 60 is combined with the data portion 62 of the database that is
11 stored in data store 44 of terminal 20 and the combination is provided to a system such as
12 navigation system 16, the system should be able to use the critical portion as a key to access the
13 data in the database. However, as noted above, the exemplary embodiment seeks to avoid some
14 of the risks associated with releasing valuable information such as geographic data. Therefore,
15 rather than simply sending the critical portion (or the entire database, if desired) to terminal 20,
16 authorization server 12 preferably first encrypts and/or otherwise secures the critical portion (or
17 entire database), producing a set of secure data, so as to avoid unauthorized use of the database.
18 Details of how this process may work in practice will be provided below.

19 At block 182, terminal 20 receives the secure data sent from authorization server 12. At
20 block 184, terminal 20 then writes to portable data storage device 22 (i) the data portion of the
21 database, which terminal 20 maintained in its data store 44, and (ii) the secure data that terminal
22 20 received from authorization server 12. As a result, at this point, data storage device 20
23 contains a secure copy of the selected database.

1 At block 186, terminal 20 then informs the user that storage device 22 is ready for use.
2 Therefore, at block 188, the user removes the storage device from communication with terminal
3 20 and, at block 190, the user communicatively couples the storage device with navigation
4 system 16. For example, if storage device 22 is a flash card, the user may insert the device into a
5 corresponding flash card socket of navigation system 16. As another example, if storage device
6 22 has a Bluetooth™ RF interface, the user may bring device 22 within an appropriate range of
7 navigation system 16 so as to couple device 22 with a corresponding data interface unit 70 of the
8 navigation system.

9 At block 192, navigation system 16 is then powered up or receives a request to provide
10 navigation services. For example, the user may engage user interface mechanism 76 in order to
11 instruct the navigation system that the user wants to travel to a specified destination address or
12 point of interest. In response, the navigation system would ordinarily retrieve geographic data
13 from data storage device 22 and use that data in combination with positioning information
14 provided by positioning system 72 to generate map 82 showing the user how to get to the
15 specified destination.

16 In the exemplary embodiment, at block 194, navigation system 16 may detect the
17 presence of device 22. In turn, at block 196, navigation system 16 may responsively seek to
18 access the database on the storage device. To do so, navigation system 16 preferably performs a
19 process to validate and/or facilitate access to the database. This process will depend on the
20 process used to secure the database. The process may be predetermined and/or may be identified
21 by a message stored on storage device 22 together with the set of secure data. Details of how
22 this process may work in practice will be provided below as well.

1 At block 198, assuming that the navigation system is precluded from accessing the
2 geographic data stored on device 22, the navigation system may audibly and/or visually alert the
3 user that navigation services are unavailable. In doing so, the navigation system may present on
4 display 74 the reasons for refusal of service. Further, in an exemplary embodiment, possibly
5 depending on the reasons for denial of service, the navigation system may send a message to a
6 central office to report the failed attempt. The navigation system may, for instance, send the
7 message over a wireless telecommunications network as an industry standard short message
8 service (SMS) message or in another manner.

9 Alternatively, at block 200, assuming that the navigation system can properly and
10 successfully access the geographic data stored on device 22, the navigation system will do so.
11 The system may then use the geographic data to provide the navigation services requested by the
12 user.

13 **C. Exemplary Securing of Data and Secure Communication of Data**

14 As noted above, the process of securing the data, and securely communicating the data,
15 can take various forms. Generally speaking, by way of example, the process may involve (i)
16 encrypting the critical portion 60 so as to establish an encrypted critical portion that can be
17 decrypted using a decryption key, (ii) establishing a set of authorization parameters useful for
18 validating and/or facilitating access to the database, and (iii) tying the authorization parameters
19 to the encrypted critical portion. At the receiving end, such as a navigation system 16, the
20 process may then involve (iv) using the authorization parameters to validate and/or facilitate
21 access to the database, (v) using the decryption key to decrypt the encrypted critical portion, and
22 then (vi) using the critical portion to facilitate access to the data portion of the database. This
23 process may facilitate securing the data, while allowing the data to be used in connection with

1 one or more authorized entities (such being stored on a given data storage medium, or being used
2 by a given navigation system, for instance). Figures 9, 10, 11 and 12 are flow charts showing
3 specific examples of how this process may work in practice.

4 Figure 9 illustrates a set of functional blocks that may be involved in securing and
5 providing data to a navigation system in accordance with an exemplary embodiment of the
6 invention. As shown in Figure 9, at block 250, the authorization server generates a random key
7 (e.g., bit string) to be associated with the selected database. (As understood in the art, it may be
8 impossible to generate a truly "random" key. However, techniques are well known for
9 generating substantially random data, and those techniques may be employed here. In this
10 regard, the term "random" may be equated with the term "substantially random.") At block 252,
11 the authorization server then uses the random key to symmetrically encrypt the critical portion 60
12 of the database, so as to produce an encrypted critical portion that can be decrypted using the
13 random key.

14 Methods of symmetric encryption are very well known in the art and others may be
15 developed in the future as well. Examples of suitable symmetric encryption methods include the
16 Advanced Encryption Standard (AES) and "Two Fish" by Bruce Schneier. Similarly, other
17 suitable methods of encryption, such as public key / private key encryption are also well known
18 in the art. Examples of such methods include elliptical curve cryptography, pretty-good-privacy
19 (PGP) and RSA. These and other encryption methods are well known to those skilled in the art
20 and are described, for instance, in Schneier, B., "Applied Cryptography -- Protocols, Algorithms,
21 and Source Code in C," Chapters 11-14, 18-19 and 24 (2d ed., John Wiley & Sons, Inc. 1996),
22 and Schneier, B. et al., "Twofish: A 128-Bit Block Cipher," <http://www.counterpane.com/twofish.html> (June 15, 1998), both of which are hereby incorporated by reference.
23

1 At block 254, the authorization server next assembles a set of authorization parameters
2 and combines the parameters to establish an authorization key that includes verification
3 information useful for validating use of the database. In the exemplary embodiment, these
4 parameters may comprise the following, for instance:

- 5 1. SYSTEM INFORMATION. These parameters may include information
6 indicating entities of the system that are authorized to possess and/or access the
7 selected database. These parameters preferably include (i) the navigation system
8 ID and (ii) the data storage ID.
- 9 2. DATABASE INFORMATION. These parameters may define information about
10 the specific database that is being provided. For instance, this information may
11 include (i) the database name, which may be indicated by a field in the database,
12 (ii) a unique serial number, which the authorization server has inserted into the
13 critical portion to identify the copy of the database, (iii) the database version (e.g.,
14 revision number) (iv) a randomly generated index into the critical portion, and the
15 32-bit value stored at that index, and (v) optional database information selected by
16 the user, such as Fodor's® Restaurant Guide, for instance.
- 17 3. DATABASE DECRYPTION KEY. This parameter is the decryption key that can
18 be used to decrypt the encrypted critical portion. Given that the authorization
19 server symmetrically encrypted the critical portion with the randomly generated
20 key, this decryption key is the randomly generated key. However, this parameter
21 may vary depending on the type of encryption performed and consequently on the
22 type of decryption required.

23

4. ACCESS LIMITATIONS. These parameters may include (i) a data range during which the database and/or a specific option is authorized to be used and (ii) a count of the number of times the database and/or option is authorized to be accessed.

5. TRACING INFORMATION. These parameters may define information that can be used by a geographic data provider to trace the source of fraudulent copies of geographic data. These parameters may include, for instance, (i) the user ID, (ii) the navigation system ID, make and model, (iii) the time and date that the authorization key is being generated, and (iv) the data terminal ID.

Alternatively, the parameters may take other forms as well. Authorization server 12 may combine these parameters together in any desired manner to establish the authorization key. For instance, assuming that each parameter can be represented as a character string or bit string, authorization server 12 can concatenate or interleave the character strings or bit strings. At block 256, the authorization server preferably also computes a CRC or checksum of the authorization key and appends or otherwise adds that CRC or checksum to the authorization key. (As used herein, the terms "CRC" and "checksum" can be considered to be equivalent. Further, other types of hash functions could also be considered to be equivalent as well.)

At block 258, the authorization server then encrypts the authorization key so as to generate an encrypted authorization key that can be decrypted with a particular decryption key. As noted above, each model of a navigation system preferably has its own private/public key pair and the encryption key to be used for the given model is preferably stored in the authorization server authorization database 40. (As further noted above, the authorization server

1 may encrypt using the private key, allowing the navigation system to decrypt using the public
2 key. Alternatively, the authorization server may encrypt using the public key, allowing the
3 navigation system to decrypt using the private key.) Thus, given the navigation system ID
4 (which may define or cross-reference to a navigation system model number, for instance), the
5 authorization server may retrieve the applicable encryption key from authorization database 40
6 and may use that encryption key to encrypt the authorization key.

7 At block 260, the authorization server then preferably sends to terminal 20 via link 18 (i)
8 the encrypted critical portion of the database and (ii) the encrypted authorization key. At block
9 262, as described above, terminal 20 may then record the encrypted critical portion, the
10 encrypted authorization key, and the data portion 62 onto data storage device 22. And, at block
11 264, a user may couple device 22 with navigation system 16.

12 Figure 10 next illustrates a set of functional blocks that may be involved in retrieval,
13 decryption and validation of the data at the navigation system. The functions performed in these
14 blocks may be performed in the interface layer software described in the '280 patent, for
15 instance, and, more particularly, in the media device isolation layer described therein. Referring
16 to Figure 10, at block 266, navigation system 16 may first read the encrypted authorization key
17 from device 22. At block 268, the navigation system will then apply its designated decryption
18 key to decrypt the encrypted authorization key so as to produce a plaintext authorization key. In
19 the exemplary embodiment, if the user tries to use the database in connection with a navigation
20 system that is not the model corresponding to the navigation system ID that the user provided,
21 the navigation system will not have the correct decryption key and therefore will not be able to
22 access the data.

1 At block 270, assuming successful decryption of the encrypted authorization key, the
2 navigation system may then use some or all of the authorization parameters to validate (i.e.,
3 establish authority to use) the database. By way of example, the navigation system may read the
4 storage device ID from the permanent memory of storage device 22 and may determine whether
5 that storage device ID matches the storage device ID provided in the authorization key. If the
6 storage device ID does not match, the navigation system may conclude that the storage device
7 contains an unauthorized copy of the database, and the navigation system may therefore refuse to
8 access the database.

9 As another example, the navigation system may determine whether its own navigation
10 system ID matches the navigation system ID provided in the authorization key. If the navigation
11 system ID does not match, the navigation system may conclude that it is not authorized to access
12 the database, and the navigation system may therefore refuse to access the database.

13 As still another example, the navigation system may use the access limitations, such as a
14 rental period or use restriction, to determine whether access is currently authorized. Specifically,
15 for example, the navigation system may determine whether the current date (as provided by the
16 GPS positioning system, for instance) falls within the date range specified in the authorization
17 key and, if the date falls outside the range, may refuse to access the database.

18 At block 272, with successful validation, the navigation system may then decrypt the
19 encrypted critical portion. In particular, the navigation system may (i) read into memory 68 from
20 the storage device 22 the encrypted critical portion, (ii) retrieve from the authorization key the
21 decryption key required for decryption of the encrypted critical portion, and (ii) use the
22 decryption key to decrypt the encrypted critical portion.

1 At block 274, the navigation system may then use the information within the critical
2 portion 60 (e.g., decompression information, indexes and pointers) as keys to access the
3 geographic data in the data portion 62. In the exemplary embodiment, the data portion remains
4 stored on data storage device 22, while the decrypted critical portion is stored in the volatile
5 memory 68 of the navigation system 16. As long as storage device 22 remains coupled with
6 navigation system 16, the navigation system may thereby continue to access the database of
7 geographical data so as to provide navigation services. When storage device 22 is removed from
8 communication with navigation system 16 or at another suitable time, the decrypted critical
9 portion is preferably cleared from memory 68, thereby preserving the security of the data
10 portion.

1 While the foregoing provides a robust method of securing geographic data, an alternative
2 process can be employed so as to provide enhanced security. In the alternative process,
3 authorization server 12 can instead symmetrically encrypt the authorization parameters and use
4 public/private key encryption to encrypt only the symmetric key, preferably together with a value
5 representative of the authorization key, rather than to encrypt the entire authorization key.
6 Figure 11 is a flow chart illustrating a set of functional blocks that may be involved in this
7 alternative process.

1 As shown in Figure 11, at block 350, the authorization server generates a random key to
2 be associated with the selected database. At block 352, the authorization server then uses the
3 random key to symmetrically encrypt the critical portion of the database, so as to produce an
4 encrypted critical portion that can be decrypted using the random key.

1 At block 354, the authorization server then assembles a set of authorization parameters
2 and combines the parameters to establish an authorization key. These parameters may be those

1 described above, for instance, including the random key necessary for decryption of the
2 encrypted critical portion.

3 At block 356, the authorization server computes a checksum or CRC, C, of the
4 authorization key. At block 358, the authorization server then generates a random value, R, and
5 uses R to symmetrically encrypt the authorization key, rather than public key encrypting the
6 authorization key.

7 At block 360, the authorization server combines together the values C and R, such as by
8 concatenating or interleaving the values for instance, to produce a value V. At block 362, the
9 authorization server uses the private key (associated with the navigation system model) to
10 encrypt the value V. Finally, at block 364, the authorization server sends to terminal 20 (i) the
11 encrypted value V, (ii) the encrypted authorization key, and (ii) the encrypted critical portion.

12 Upon receipt of this information, at block 366, terminal 20 then preferably records onto
13 data storage device, (i) the encrypted value V, (ii) the encrypted authorization key, (iii) the
14 encrypted critical portion, and (iv) the unintelligible data portion of the database.

15 When the navigation system receives data storage device 22 and seeks to access the
16 database, at block 368, the navigation system uses its public key to decrypt the encrypted value
17 V. The navigation system may therefore retrieve values R and C from value V. At block 370,
18 the navigation system then uses value R to symmetrically decrypt the encrypted authorization
19 key. At block 372, the navigation system then computes the checksum or CRC of the
20 authorization key and compares the resulting value with value C. If value C matches, then, at
21 block 374, the navigation system proceeds to use the authorization parameters to validate use of
22 the database as described above. Alternatively, if value C does not match, then, at block 376, the
23 navigation system may refuse to access the geographic database.

1 In yet another exemplary embodiment, the process of securing geographic data can be
2 still further enhanced. In this further embodiment, the authorization key can be encrypted in
3 such a way that the decryption key required to access the authorization key is itself tied to
4 environmental parameters, such as the authorization parameters and/or contents of the database.
5 Figure 12 is a flow chart depicting an example of this further enhanced security process.

6 As shown in Figure 12, at block 450, the authorization server generates a random value,
7 K, and uses the value K as a key to symmetrically encrypt the critical portion of the database, so
8 as to produce an encrypted critical portion that can be decrypted using the value K.

9 At block 452, the authorization server then assembles a set of authorization parameters
10 and combines the parameters to establish an authorization key. These parameters may be the
11 same as those described above, except that the parameters preferably exclude the navigation
12 system ID and the storage device ID. The navigation system ID and storage device ID will
13 instead be used in the process of producing a symmetric key for encrypting the authorization key.
14 Further, the parameters preferably do not yet include the value K required for decryption of the
15 encrypted critical portion of the database. Still further, the parameters may exclude the database
16 version information and other such information (since, as will be noted below, other intrinsic
17 information about the database (e.g., bytes of the database) may be incorporated in the securing
18 process instead).

19 At block 454, the authorization server calculates a checksum or CRC, C, of the
20 authorization key. At block 456, the authorization server may then generate an ID value, N,
21 which the authorization server may record in its data store 28 as a key to a database record
22 indicative of environmental parameters such as the user, the navigation system and the storage
23 device for instance.

1 Next, at block 458, the authorization server computes a one-way hash function or other
2 function to generate an output value H. The hash function is preferably based on the
3 authorization key. In particular, for instance, the inputs to the hash function are preferably
4 values that should be accessible by both the machine generating the authorization key (i.e.,
5 authorization server 12) and the machine that will decrypt the authorization key (i.e., navigation
6 system 16). In this exemplary embodiment, the inputs to the hash function include
7 environmental parameters, such as (i) the navigation system ID, (ii) the storage device ID, (iii)
8 the ID value N, (iv) the checksum or CRC value C, and (v) a predetermined number of bytes
9 selected from a predetermined location of the encrypted critical portion of the database. Suitable
10 hash functions are well known to those skilled in the art, as described, for instance, in Schneier,
11 B., "Applied Cryptography -- Protocols, Algorithms, and Source Code in C," Chapters 11-14,
12 18-19 and 24 (2d ed., John Wiley & Sons, Inc. 1996).

13 At block 460, the authorization server may then XOR or otherwise combine the output
14 value H with the random value K that was used to symmetrically encrypt the critical portion of
15 the database, and the authorization server may thereby produce a value K'. At block 462, the
16 authorization server may then append or otherwise add the value K' to the authorization key.
17 This way, a machine seeking to access the database will be forced to first establish the value H
18 and then XOR the value H with the value K', so as to recover the value K for use in decrypting
19 the encrypted critical portion. Therefore, the machine seeking access to the data will need to
20 have access to the parameters that were used to establish the value H (such as navigation system
21 ID and storage device ID, for instance) in order for the machine to effectively have access to the
22 decryption key K, in order to facilitate decryption of the critical portion and, in turn, in order to
23 facilitate access to the database.

1 At block 464, the authorization server preferably uses the value H as a symmetric key to
2 encrypt the authorization key, so as to produce an encrypted authorization key that can be
3 decrypted using the value H. Again, because the value H stems from certain environmental
4 parameters such as the navigation system ID and storage device ID, for instance, a machine
5 seeking access to the database will need to know these parameters in order to facilitate access to
6 the database, thereby providing added security.

7 At block 466, the authorization server may next combine together the ID value N with the
8 checksum or CRC value C, such as by concatenating or interleaving the values for instance, to
9 produce a value V. At block 468, the authorization server then uses the private key (associated
10 with the navigation system model) to encrypt the value V. Finally, at block 470, the
11 authorization server sends to terminal 20 (i) the encrypted value V, (ii) the encrypted
12 authorization key, and (ii) the encrypted critical portion.

13 Upon receipt of this information, at block 472, terminal 20 then preferably records onto
14 data storage device, (i) the encrypted value V, (ii) the encrypted authorization key, (iii) the
15 encrypted critical portion, and (iv) the unintelligible data portion of the database.

16 When the navigation system receives data storage device 22 and seeks to access the
17 database, at block 474, the navigation system uses its public key to decrypt the encrypted value
18 V. The navigation system may therefore retrieve values N and C from value V.

19 At block 476, the navigation system then computes the same hash function that the
20 authorization server computed, with the same inputs used by the authorization server. In the
21 exemplary embodiment, therefore, if navigation system does not have access to the
22 environmental parameters, such as the navigation system ID and storage device ID, the
23 navigation system will not be able to successfully compute the same value H that the

1 authorization server computed, and the navigation system may be precluded from accessing the
2 database. Similarly, if the navigation system does not have the required public key and is
3 therefore unable to decrypt encrypted value V at block 474, it will not be able to uncover values
4 N and C and, consequently, it will not be able to compute the hash function. However, if the
5 navigation system has access to, and uses, the appropriate inputs, the hash function will produce
6 the value H.

7 At block 478, the navigation system then uses the computed value H as a symmetric key
8 to decrypt the encrypted authorization key. In turn, at block 480, the navigation system
9 computes the checksum or CRC of the authorization key and compares that value to the value C
10 that it retrieved from the value V. If value C does not match, then, at block 482, the navigation
11 system may refuse to access the database. Alternatively, if value C matches, then the navigation
12 system continues to block 484. At block 484, the navigation system extracts from the
13 authorization key the value K', and, at block 486, the navigation system XORs or otherwise
14 combines K' with H so as to reveal the value K.

15 At block 488, the navigation system may use other parameters of the authorization key to
16 validate use of the database. Finally, assuming successful validation, at block 490, the
17 navigation system may use the value K as a symmetric key to decrypt the encrypted critical
18 portion of the database and may proceed to access and use the data portion of the database.

19 In still a further exemplary embodiment, the process of securing geographic data can be
20 additionally enhanced, still tying the authorization key to environmental parameters. In this
21 further embodiment, the authorization server may first generate a random number K and may
22 then use that random number K as a key to symmetrically encrypt the critical portion of the
23 database. The authorization server may then compile a first portion A' of an authorization key,

1 including parameters such as a pointer to a randomly selected location of the database and a
2 value at that location, starting and ending dates for data validity, maximum use count, and
3 information about selected options. The authorization server may also include in the first portion
4 A' one or more values computed as a one-way hash function of the critical portion of the
5 database.

6 The authorization server may then apply a one-way hash function, whose inputs may be
7 the navigation system ID, the storage device ID, the first portion A' of the authorization key,
8 some number of bytes from the encrypted critical portion, and/or other parameters that may be
9 accessible by both the navigation system and the authorization server. The output of the hash
10 function may be designated H.

11 The authorization server may then XOR the output H with the random number K, so as to
12 produce a value K'. In turn, the authorization server may store the value K' in a second portion
13 A" of the authorization key. The authorization server may then calculate a CRC or hash function
14 of A' and K' (or perhaps just a CRC or hash function of just A') and store the result in the second
15 portion A" as well.

16 Next, the authorization server may append or otherwise combine together A' and A" to
17 produce an authorization key A. The authorization server may then encrypt the authorization
18 key with the navigation system's private key (or public key). Finally, the authorization server
19 may send to terminal 20 the symmetrically encrypted critical portion of the database and the
20 encrypted authorization key.

21 Upon receipt of this information, terminal 20 may record the information onto the data
22 storage device 22, together with the unintelligible portion of the database. Thereafter, when the
23 data storage device is coupled with the navigation system, the navigation system may use its

1 public key (or private key) to decrypt the encrypted authorization key, so as to recover the
2 plaintext authorization key A.

3 The navigation system may then compute the same CRC or hash function of A and K'
4 that the authorization server computed and may compare the result with the value stored in the
5 second portion A" of the authorization key. If the values do not match, then the navigation
6 system may be programmed to abort its efforts to access the data.

7 The navigation system may next check to ensure that the current date is between the
8 starting and ending dates provided in the first portion A' of the authorization key. If the current
9 date does not fall within the allowed date range, then the navigation system may also be
10 programmed to abort.

11 The navigation system may then compute the same hash function that the authorization
12 server computed, with the same inputs used by the authorization server, so as to produce the
13 output H. In turn, the navigation system may XOR the value H with the value K' that is stored in
14 the second portion A" of the authorization key, so as to recover the value K. Thereafter, the
15 navigation system may use the value K as a key to symmetrically decrypt the encrypted critical
16 portion of the database and may then proceed to access and use the data portion of the database.

17 In this exemplary embodiment, the navigation system would therefore need to have
18 access to environmental parameters such as the navigation system ID and storage device ID as
19 used in the hash function computed by the authorization server. Absent access to such
20 information, the navigation system would be prevented from computing the value H, which
21 would prevent the navigation system from uncovering the value K needed to symmetrically
22 decrypt the critical portion of the database.

1 Further, in an arrangement where the authorization server included in first portion A' one
2 or more hash values of the critical portion of the database, the navigation system may be
3 programmed to verify those hash values by computing the same hash function as applied by the
4 authorization server and comparing the resulting values.

5 **D. Exemplary Advantages**

6 The system and method described by way of example in this specification can
7 advantageously help avoid many of the security risks associated with providing valuable data,
8 such as geographic data. For instance, in various embodiments, the system and method can help
9 foil attempts at fraud in the following manners:

- 10 1. If someone tries to copy the data to another storage device, the machine seeking
11 to access the data may determine that the storage device is not authorized to hold
12 the data and may therefore refuse to access the data.
13 2. If someone tries to access the data using a machine other than the authorized
14 machine, the machine may determine that it is not authorized to access the data
15 and may therefore refuse to access the data.
16 3. If someone tries to use the authorization key to access data other than the data for
17 which the authorization key was generated, access may be precluded.
18 4. If someone tries to use an expired set of data (such as a database for which a
19 rental period or number of uses has expired), access may be precluded.
20 5. If someone tries to access the data using a machine that is not programmed to
21 perform validation, access may be precluded.

22 In addition, the exemplary embodiments provide additional security features. For
23 example, a random encryption key is used for each instance of a database, thereby helping to

1 prevent certain types of cryptanalysis. As another example, by tying authorization to database
2 access libraries (e.g., the critical portion of a database), authorization becomes required in order
3 to access the database. Therefore, navigation system vendor may have to include authorization
4 functions in their systems.

5 **E. Alternative Embodiment**

6 In an alternative embodiment of the present invention, some or all of the geographic data
7 or authorization information can be provided more directly from the authorization server to the
8 navigation system. Figure 13 is a simplified block diagram illustrating this alternative
9 embodiment by way of example.

10 In this alternative embodiment, as shown in Figure 13, a communications link 14 couples
11 the authorization server 12 to a representative navigation system 16. Link 14 may take any form
12 suitable for carrying communications between authorization server 12 and navigation system 16.
13 For instance, link 14 may include or take the form of a satellite or cellular communications
14 system or other wireless interface and/or the public switched telephone network or other landline
15 interface. As such, link 14 may include various intermediate elements as well (not shown in
16 Figure 13).

17 In this embodiment, the data interface units 32, 70 of authorization server 12 and
18 navigation system 16 then take a form suitable for communicating with link 14. Alternatively,
19 authorization server 12 and/or navigation system 16 each include an additional data interface unit
20 suitable for communicating with link 14. For instance, if link 14 is a cellular
21 telecommunications network, then navigation system 16 preferably includes the components that
22 would ordinarily be found within a cellular telephone or other mobile station (such as an

1 appropriate RF transceiver and the program logic necessary to originate and terminate calls, for
2 example).

3 In this embodiment, authorization server 12 can itself convey the entire secured
4 geographic database to navigation system 16 via link 14. In particular, authorization server 12
5 preferably prepares and provides to navigation system 16 (i) the authorization material (e.g.,
6 encrypted critical portion and authorization parameters, etc.) described above as being provided
7 by authorization server 12 to data distribution terminal 20 and (ii) the data portion 62 of a
8 geographic database to be used by the navigation system 16. The authorization server may
9 provide this material to the navigation system on request or in response to another specified
B0 stimulus. Further, in the event the navigation system already has the data portion 62 of a given
B1 database, the authorization server may conveniently send only the authorization material to the
B2 navigation system. The navigation system 16 may then employ a process equivalent to that
B3 described above, to decrypt, validate and use the database.

As shown in Figure 13, communications link 18, data terminal 20, and portable data
storage device 22 may also still be employed to carry information from authorization server 12 to
navigation system 16 in this alternative embodiment. In this arrangement, for instance, some
information may be conveyed via link 14 to the navigation system 16, and other information may
be conveyed via link 18 to data terminal 20 and then via portable storage device 22 to navigation
system 16.

As a particular example, a user may load the data portion 62 of a database onto storage
device 22 at terminal 20, for instance, and then couple the storage device with a navigation
system 16. In providing the user with the data portion 62, terminal 20 may communicate with
authorization server 12 to an extent as provided above, and authorization server 12 may establish

1 the necessary authorization material (e.g., encrypted critical portion and authorization
2 parameters, etc.) Unlike the above scenario, however, authorization server 12 might not send the
3 authorization material to terminal 20. When navigation system 16 then detects the presence of
4 the storage device 22, it may be programmed to responsively contact authorization server 12 via
5 link 14 (e.g., by placing a cellular telephone call to the authorization server) and to request the
6 authorization material. Authorization server 12 may then send the authorization material, and
7 navigation system 16 may use the authorization material to facilitate access to the database.

8 As still another variation of this alternative embodiment, link 14 may itself comprise
9 portable data storage device 22, which may be physically transported from authorization server
10 12 (or another entity) to navigation system 16. In this arrangement, for instance, authorization
11 server 12 may record onto storage device 22 all of the information that terminal 20 would have
12 recorded onto the storage device in the embodiments described above and then provide the
13 storage device for use in navigation system 16.

14 In this variation, for instance, a user may order a particular set of geographic data from a
15 data provider, such as via the Internet or via a call center. The data provider may obtain the user
16 ID, navigation system ID and other information (such as the information that terminal 20 would
17 obtain in the embodiments described above) and then employ the authorization server to generate
18 and record onto a storage device 22 the requested data set. The data provider may then ship or
19 otherwise transport the loaded storage device 22 to the user for use by the navigation system as
20 described above.

21 **F. Conclusion**

22 Examples of the present invention have been described above. Those skilled in the art will
23 understand, however, that changes and modifications may be made in these embodiments without

1 departing from the true scope and spirit of the present invention, which is defined by the following
2 claims.

3 For example, where the above description notes that certain logic functions may be
4 carried out by a processor executing software instructions, those functions can equally be
5 employed through hardware, firmware, or a combination of hardware, firmware and software if
6 desired.

7 As another example, while the foregoing description has focused on securing geographic
8 data and providing geographic data for use by a navigation system, the elements, systems and
9 processes described can be equally employed to secure and communicate other types of data for
10 use in other contexts. Examples of such other data include those described in the background
11 section (e.g., data for music players or video players (such as songs or movies), data for video
12 game consoles (such as games, etc.), as well as other sorts of data now known or later developed.

CLAIMS

I claim:

1 1. A method for on-line mass distribution of data products to end users, the method
2 comprising:

3 maintaining a first portion of each of said data products at a first location;

4 maintaining a second portion of each of said data products at a second location;

5 for each of said end users, confirming the end user's entitlement to one of said data

6 products;

7 obtaining a first portion of said one of said data products from said first location and a
8 second portion of said one of said data products from said second location;

9 combining said first portion of said one of said data products and said second portion of
10 said one of said data products; and

11 providing said combined first portion and second portion to said user.

12 2. The method of claim 1, wherein said data products include geographic databases.

13 3. The method of claim 1, wherein said data products include digital copies of
14 movies.

15 4. The method of claim 1, wherein said data products include digital copies of
16 musical songs.

1 5. The method of claim 1, further comprising the step of:
2 encrypting said first portion of each of said data products.
3

1 6. The method of claim 1, further comprising the step of:
2 prior to the step of combining, encrypting said first portion of one of said data products.
3

1 7. The method of claim 1, wherein said step of combining is performed at said
2 second location.
3

1 8. A system for secure on-line mass distribution of data products to end users
2 comprising:

3 an authorization server having associated therewith copies of first portions of a plurality
4 of data products;

5 a plurality of data distribution terminals, each of which has associated therewith copies of
6 second portions of said plurality of data products;

7 a communications system that provides for exchange of data between said authorization
8 server and said plurality of data distribution terminals, and

9 a data distribution program that provides copies of said data products to those end users
10 who are entitled to have said copies thereof, wherein said data distribution program provides a
11 copy of a data product by combining a copy of the first portion of said data product obtained
12 from said authorization server with a copy of the second portion of said data product obtained
13 from one of said plurality of data distribution terminals.

1 9. The system of claim 8, wherein said authorization server also has associated
2 therewith an authorization database containing data indicating entitlement by said end users to
3 copies of said data products.

4

1 10. A system for securely conveying a data product, the data product defining a first
2 portion and a second portion, the first portion defining at least one key to the second portion, the
3 system comprising, in combination:

4 a first entity maintaining the first portion;

5 a second entity maintaining the second portion;

6 a first set of logic executable by the first entity to encrypt the first portion so as to
7 produce an encrypted first portion that can be decrypted using a first decryption key, wherein the
8 first entity sends the encrypted first portion via a telecommunications link to the second entity;
9 and

10 a second set of logic executable by the second entity, upon receipt of the encrypted first
11 portion, to record onto a storage medium the encrypted first portion and the second portion,

12 wherein the storage medium may be provided to a third entity, which, if provided with
13 access to the first decryption key, can in turn access the data product.

14

1 11. The system of claim 10, wherein the first entity sends to the second entity,
2 together with the encrypted first portion, an encrypted authorization key that can be decrypted
3 using a second decryption key so as to reveal verification information indicative of an entity
4 authorized to access the data product, and wherein the second set of logic is further executable to
5 record onto the storage medium the encrypted authorization key.

1 12. The system of claim 11, wherein the second decryption key is derived as a
2 function of an environmental parameter.

3

1 13. The system of claim 12, wherein the environmental parameter comprises an
2 identification code associated with the entity authorized to access the data product.

3

1 14. The system of claim 11, wherein the third entity has access to the second
2 decryption key, the system further comprising:

3 a third set of logic executable by the third entity to decrypt the encrypted authorization
4 key, to thereby gain access to the verification information, and to use the verification information
5 to validate use of the data product.

B6
B5
B4
B3
B2
B1
A2
A1
P1
P2
P3
P4
P5
P6
P7
P8
P9
P10
P11
P12
P13
P14
P15
P16
P17
P18
P19
P20
P21
P22
P23
P24
P25
P26
P27
P28
P29
P30
P31
P32
P33
P34
P35
P36
P37
P38
P39
P40
P41
P42
P43
P44
P45
P46
P47
P48
P49
P50
P51
P52
P53
P54
P55
P56
P57
P58
P59
P60
P61
P62
P63
P64
P65
P66
P67
P68
P69
P70
P71
P72
P73
P74
P75
P76
P77
P78
P79
P80
P81
P82
P83
P84
P85
P86
P87
P88
P89
P90
P91
P92
P93
P94
P95
P96
P97
P98
P99
P100
P101
P102
P103
P104
P105
P106
P107
P108
P109
P110
P111
P112
P113
P114
P115
P116
P117
P118
P119
P120
P121
P122
P123
P124
P125
P126
P127
P128
P129
P130
P131
P132
P133
P134
P135
P136
P137
P138
P139
P140
P141
P142
P143
P144
P145
P146
P147
P148
P149
P150
P151
P152
P153
P154
P155
P156
P157
P158
P159
P159
P160
P161
P162
P163
P164
P165
P166
P167
P168
P169
P170
P171
P172
P173
P174
P175
P176
P177
P178
P179
P180
P181
P182
P183
P184
P185
P186
P187
P188
P189
P190
P191
P192
P193
P194
P195
P196
P197
P198
P199
P200
P201
P202
P203
P204
P205
P206
P207
P208
P209
P209
P210
P211
P212
P213
P214
P215
P216
P217
P218
P219
P219
P220
P221
P222
P223
P224
P225
P226
P227
P228
P229
P229
P230
P231
P232
P233
P234
P235
P236
P237
P238
P239
P239
P240
P241
P242
P243
P244
P245
P246
P247
P248
P249
P249
P250
P251
P252
P253
P254
P255
P256
P257
P258
P259
P259
P260
P261
P262
P263
P264
P265
P266
P267
P268
P269
P269
P270
P271
P272
P273
P274
P275
P276
P277
P278
P279
P279
P280
P281
P282
P283
P284
P285
P286
P287
P288
P289
P289
P290
P291
P292
P293
P294
P295
P296
P297
P298
P299
P299
P300
P301
P302
P303
P304
P305
P306
P307
P308
P309
P309
P310
P311
P312
P313
P314
P315
P316
P317
P318
P319
P319
P320
P321
P322
P323
P324
P325
P326
P327
P328
P329
P329
P330
P331
P332
P333
P334
P335
P336
P337
P338
P339
P339
P340
P341
P342
P343
P344
P345
P346
P347
P348
P349
P349
P350
P351
P352
P353
P354
P355
P356
P357
P358
P359
P359
P360
P361
P362
P363
P364
P365
P366
P367
P368
P369
P369
P370
P371
P372
P373
P374
P375
P376
P377
P378
P379
P379
P380
P381
P382
P383
P384
P385
P386
P387
P388
P389
P389
P390
P391
P392
P393
P394
P395
P396
P397
P398
P399
P399
P400
P401
P402
P403
P404
P405
P406
P407
P408
P409
P409
P410
P411
P412
P413
P414
P415
P416
P417
P418
P419
P419
P420
P421
P422
P423
P424
P425
P426
P427
P428
P429
P429
P430
P431
P432
P433
P434
P435
P436
P437
P438
P439
P439
P440
P441
P442
P443
P444
P445
P446
P447
P448
P449
P449
P450
P451
P452
P453
P454
P455
P456
P457
P458
P459
P459
P460
P461
P462
P463
P464
P465
P466
P467
P468
P469
P469
P470
P471
P472
P473
P474
P475
P476
P477
P478
P479
P479
P480
P481
P482
P483
P484
P485
P486
P487
P488
P489
P489
P490
P491
P492
P493
P494
P495
P496
P497
P498
P499
P499
P500
P501
P502
P503
P504
P505
P506
P507
P508
P509
P509
P510
P511
P512
P513
P514
P515
P516
P517
P518
P519
P519
P520
P521
P522
P523
P524
P525
P526
P527
P528
P529
P529
P530
P531
P532
P533
P534
P535
P536
P537
P538
P539
P539
P540
P541
P542
P543
P544
P545
P546
P547
P548
P549
P549
P550
P551
P552
P553
P554
P555
P556
P557
P558
P559
P559
P560
P561
P562
P563
P564
P565
P566
P567
P568
P569
P569
P570
P571
P572
P573
P574
P575
P576
P577
P578
P579
P579
P580
P581
P582
P583
P584
P585
P586
P587
P588
P589
P589
P590
P591
P592
P593
P594
P595
P596
P597
P598
P599
P599
P600
P601
P602
P603
P604
P605
P606
P607
P608
P609
P609
P610
P611
P612
P613
P614
P615
P616
P617
P618
P619
P619
P620
P621
P622
P623
P624
P625
P626
P627
P628
P629
P629
P630
P631
P632
P633
P634
P635
P636
P637
P638
P639
P639
P640
P641
P642
P643
P644
P645
P646
P647
P648
P649
P649
P650
P651
P652
P653
P654
P655
P656
P657
P658
P659
P659
P660
P661
P662
P663
P664
P665
P666
P667
P668
P669
P669
P670
P671
P672
P673
P674
P675
P676
P677
P678
P679
P679
P680
P681
P682
P683
P684
P685
P686
P687
P688
P689
P689
P690
P691
P692
P693
P694
P695
P696
P697
P698
P699
P699
P700
P701
P702
P703
P704
P705
P706
P707
P708
P709
P709
P710
P711
P712
P713
P714
P715
P716
P717
P718
P719
P719
P720
P721
P722
P723
P724
P725
P726
P727
P728
P729
P729
P730
P731
P732
P733
P734
P735
P736
P737
P738
P739
P739
P740
P741
P742
P743
P744
P745
P746
P747
P748
P749
P749
P750
P751
P752
P753
P754
P755
P756
P757
P758
P759
P759
P760
P761
P762
P763
P764
P765
P766
P767
P768
P769
P769
P770
P771
P772
P773
P774
P775
P776
P777
P778
P779
P779
P780
P781
P782
P783
P784
P785
P786
P787
P788
P789
P789
P790
P791
P792
P793
P794
P795
P796
P797
P798
P799
P799
P800
P801
P802
P803
P804
P805
P806
P807
P808
P809
P809
P810
P811
P812
P813
P814
P815
P816
P817
P818
P819
P819
P820
P821
P822
P823
P824
P825
P826
P827
P828
P829
P829
P830
P831
P832
P833
P834
P835
P836
P837
P838
P839
P839
P840
P841
P842
P843
P844
P845
P846
P847
P848
P849
P849
P850
P851
P852
P853
P854
P855
P856
P857
P858
P859
P859
P860
P861
P862
P863
P864
P865
P866
P867
P868
P869
P869
P870
P871
P872
P873
P874
P875
P876
P877
P878
P879
P879
P880
P881
P882
P883
P884
P885
P886
P887
P888
P889
P889
P890
P891
P892
P893
P894
P895
P896
P897
P898
P899
P899
P900
P901
P902
P903
P904
P905
P906
P907
P908
P909
P909
P910
P911
P912
P913
P914
P915
P916
P917
P918
P919
P919
P920
P921
P922
P923
P924
P925
P926
P927
P928
P929
P929
P930
P931
P932
P933
P934
P935
P936
P937
P938
P939
P939
P940
P941
P942
P943
P944
P945
P946
P947
P948
P949
P949
P950
P951
P952
P953
P954
P955
P956
P957
P958
P959
P959
P960
P961
P962
P963
P964
P965
P966
P967
P968
P969
P969
P970
P971
P972
P973
P974
P975
P976
P977
P978
P979
P979
P980
P981
P982
P983
P984
P985
P986
P987
P988
P989
P989
P990
P991
P992
P993
P994
P995
P996
P997
P998
P999
P999
P1000
P1001
P1002
P1003
P1004
P1005
P1006
P1007
P1008
P1009
P1009
P1010
P1011
P1012
P1013
P1014
P1015
P1016
P1017
P1018
P1019
P1019
P1020
P1021
P1022
P1023
P1024
P1025
P1026
P1027
P1028
P1029
P1029
P1030
P1031
P1032
P1033
P1034
P1035
P1036
P1037
P1038
P1039
P1039
P1040
P1041
P1042
P1043
P1044
P1045
P1046
P1047
P1048
P1049
P1049
P1050
P1051
P1052
P1053
P1054
P1055
P1056
P1057
P1058
P1059
P1059
P1060
P1061
P1062
P1063
P1064
P1065
P1066
P1067
P1068
P1069
P1069
P1070
P1071
P1072
P1073
P1074
P1075
P1076
P1077
P1078
P1079
P1079
P1080
P1081
P1082
P1083
P1084
P1085
P1086
P1087
P1088
P1089
P1089
P1090
P1091
P1092
P1093
P1094
P1095
P1096
P1097
P1098
P1099
P1099
P1100
P1101
P1102
P1103
P1104
P1105
P1106
P1107
P1108
P1109
P1109
P1110
P1111
P1112
P1113
P1114
P1115
P1116
P1117
P1118
P1119
P1119
P1120
P1121
P1122
P1123
P1124
P1125
P1126
P1127
P1128
P1129
P1129
P1130
P1131
P1132
P1133
P1134
P1135
P1136
P1137
P1138
P1139
P1139
P1140
P1141
P1142
P1143
P1144
P1145
P1146
P1147
P1148
P1149
P1149
P1150
P1151
P1152
P1153
P1154
P1155
P1156
P1157
P1158
P1159
P1159
P1160
P1161
P1162
P1163
P1164
P1165
P1166
P1167
P1168
P1169
P1169
P1170
P1171
P1172
P1173
P1174
P1175
P1176
P1177
P1178
P1179
P1179
P1180
P1181
P1182
P1183
P1184
P1185
P1186
P1187
P1188
P1189
P1189
P1190
P1191
P1192
P1193
P1194
P1195
P1196
P1197
P1198
P1199
P1199
P1200
P1201
P1202
P1203
P1204
P1205
P1206
P1207
P1208
P1209
P1209
P1210
P1211
P1212
P1213
P1214
P1215
P1216
P1217
P1218
P1219
P1219
P1220
P1221
P1222
P1223
P1224
P1225
P1226
P1227
P1228
P1229
P1229
P1230
P1231
P1232
P1233
P1234
P1235
P1236
P1237
P1238
P1239
P1239
P1240
P1241
P1242
P1243
P1244
P1245
P1246
P1247
P1248
P1249
P1249
P1250
P1251
P1252
P1253
P1254
P1255
P1256
P1257
P1258
P1259
P1259
P1260
P1261
P1262
P1263
P1264
P1265
P1266
P1267
P1268
P1269
P1269
P1270
P1271
P1272
P1273
P1274
P1275
P1276
P1277
P1278
P1279
P1279
P1280
P1281
P1282
P1283
P1284
P1285
P1286
P1287
P1288
P1289
P1289
P1290
P1291
P1292
P1293
P1294
P1295
P1296
P1297
P1298
P1299
P1299
P1300
P1301
P1302
P1303
P1304
P1305
P1306
P1307
P1308
P1309
P1309
P1310
P1311
P1312
P1313
P1314
P1315
P1316
P1317
P1318
P1319
P1319
P1320
P1321
P1322
P1323
P1324
P1325
P1326
P1327
P1328
P1329
P1329
P1330
P1331
P1332
P1333
P1334
P1335
P1336
P1337
P1338
P1339
P1339
P1340
P1341
P1342
P1343
P1344
P1345
P1346
P1347
P1348
P1349
P1349
P1350
P1351
P1352
P1353
P1354
P1355
P1356
P1357
P1358
P1359
P1359
P1360
P1361
P1362
P1363
P1364
P1365
P1366
P1367
P1368
P1369
P1369
P1370
P1371
P1372
P1373
P1374
P1375
P1376
P1377
P1378
P1379
P1379
P1380
P1381
P1382
P1383
P1384
P1385
P1386
P1387
P1388
P1389
P1389
P1390
P1391
P1392
P1393
P1394
P1395
P1396
P1397
P1398
P1399
P1399
P1400
P1401
P1402
P1403
P1404
P1405
P1406
P1407
P1408
P1409
P1409
P1410
P1411
P1412
P1413
P1414
P1415
P1416
P1417
P1418
P1419
P1419
P1420
P1421
P1422
P1423
P1424
P1425
P1426
P1427
P1428
P1429
P1429
P1430
P1431
P1432
P1433
P1434
P1435
P1436
P1437
P1438
P1439
P1439
P1440
P1441
P1442
P1443
P1444
P1445
P1446
P1447
P1448
P1449
P1449
P1450
P1451
P1452
P1453
P1454
P1455
P1456
P1457
P1458
P1459
P1459
P1460
P1461
P1462
P1463
P1464
P1465
P1466
P1467
P1468
P1469
P1469
P1470
P1471
P1472
P1473
P1474
P1475
P1476
P1477
P1478
P1479
P1479
P1480
P1481
P1482
P1483
P1484
P1485
P1486
P1487
P1488
P1489
P1489
P1490
P1491
P1492
P1493
P1494
P1495
P1496
P1497
P1498
P1499
P1499
P1500
P1501
P1502
P1503
P1504
P1505
P1506
P1507
P1508
P1509
P1509
P1510
P1511
P1512
P1513
P1514
P1515
P1516
P1517
P1518
P1519
P1519
P1520
P1521
P1522
P1523
P1524
P1525
P1526
P1527
P1528
P1529
P1529
P1530
P1531
P1532
P1533
P1534
P1535
P1536
P1537
P1538
P1539
P1539
P1540
P1541
P1542
P1543
P1544
P1545
P1546
P1547
P1548
P1549
P1549
P1550
P1551
P1552
P1553
P1554
P1555
P1556
P1557
P1558
P1559
P1559
P1560
P1561
P1562
P1563
P1564
P1565
P1566
P1567
P1568
P1569
P1569
P1570
P1571
P1572
P1573
P1574
P1575
P1576
P1577
P1578
P1579
P1579
P1580
P1581
P1582
P1583
P1584
P1585
P1586
P1587
P1588
P1589
P1589
P1590
P1591
P1592
P1593
P1594
P1595

1 17. The system of claim 10, wherein the first entity sends to the second entity,
2 together with the encrypted first portion, an encrypted authorization key that can be decrypted
3 using a second decryption key so as to reveal verification information indicative of an entity
4 authorized to store the data product.

5

1 18. The system of claim 17, wherein the second decryption key is derived as a
2 function of an environmental parameter.

3

1 19. The system of claim 18, wherein the environmental parameter comprises an
2 identification code associated with the entity authorized to store the data product.

卷之三

20. The system of claim 17, wherein the third entity has access to the second decryption key, the system further comprising:

a third set of logic executable by the third entity to decrypt the encrypted authorization key, to thereby gain access to the verification information, and to use the verification information to validate storage of the data product.

6

1 21. The system of claim 17, wherein the third entity has access to the second
2 decryption key, the system further comprising:

3 a third set of logic executable by the third entity to decrypt the encrypted authorization
4 information, to thereby gain access to the verification information, and to compare at least a
5 portion of the verification information to predetermined information associated with the storage
6 medium so as to determine whether the storage medium is authorized to store the data product.

1 22. The system of claim 21, wherein the predetermined information associated with
2 the storage medium comprises an identification code.

3

1 23. The system of claim 10, wherein the data product comprises geographic
2 information and the third entity comprises a navigation system.

3

1 24. A method for securely conveying a data product, the data product defining a first
2 portion and a second portion, the first portion defining at least one key to the second portion, the
3 method comprising, in combination:

4 at a first entity, encrypting the first portion of the data product so as to produce an
5 encrypted first portion that can be decrypted using a first decryption key;

6 sending the encrypted first portion via a telecommunications link from the first entity to a
7 second entity;

8 receiving the encrypted first portion at the second entity;

9 at the second entity, recording onto a storage medium the encrypted first portion and the
10 second portion; and

11 thereafter providing the storage medium to a third entity,

12 whereby, if the third entity has access to the first decryption key, the third entity may
13 decrypt the encrypted first portion and thereby gain access to the data product.

14

1 25. The method of claim 24, further comprising sending to the second entity, together
2 with the encrypted first portion, an encrypted authorization key that can be decrypted using a

3 second decryption key so as to reveal verification information indicative of an entity authorized
4 to access the data product.

5

1 26. The method of claim 25, further comprising generating the second decryption key
2 as a function of an environmental parameter.

3

1 27. The method of claim 26, wherein the environmental parameter comprises an
2 identification code associated with the entity authorized to access the data product.

3

1 28. The method of claim 27, further comprising:
2 the third entity generating the second decryption key as the function of the identification
3 code;
4 the third entity using the second decryption key to decrypt the encrypted authorization
5 key and to thereby gain access to the verification information; and
6 the third entity using the verification information to validate storage of the data product.

7
1 29. The method of claim 25, further comprising:

2 the third entity using the second decryption key to decrypt the encrypted authorization
3 key and to thereby gain access to the verification information; and
4 the third entity using the verification information to validate use of the data product.

5

1 30. The method of claim 29, wherein using the verification information to validate
2 use of the data product comprises comparing at least a portion of the verification information to
3 predetermined information associated with the third entity so as to determine whether the third
4 entity is authorized to access the data product.

5

1 31. The method of claim 30, wherein the predetermined information associated with
2 the third entity comprises an identification code.

3

1 32. The method of claim 24, further comprising sending to the second entity, together
2 with the encrypted first portion, an encrypted authorization key that can be decrypted using a
3 second decryption key so as to reveal verification information indicative of an entity authorized
4 to store the data product.

卷之三

25

卷之三

卷之三

1

1 34. The method of claim 33, wherein the environmental parameter comprises an
2 identification code associated with the entity authorized to store the data product.

3

1 35. The method of claim 34, further comprising:
2 the third entity generating the second decryption key as the function of the identification
3 code;
4 the third entity using the second decryption key to decrypt the encrypted authorization
5 key and to thereby gain access to the verification information; and
6 the third entity using the verification information to validate storage of the data product.

7

1 36. The method of claim 32, further comprising:
2 the third entity using the second decryption key to decrypt the encrypted authorization
3 key and to thereby gain access to the verification information; and
4 the third entity using the verification information to validate storage of the data product.

5

1 37. The method of claim 36, wherein using the verification information to validate
2 storage of the data product comprises comparing at least a portion of the verification information
3 to predetermined information associated with the storage medium so as to determine whether the
4 storage medium is authorized to store the data product.

5

1 38. The method of claim 37, wherein the predetermined information associated with
2 the storage medium comprises an identification code.

3

1 39. The method of claim 24, wherein the data product comprises geographic
2 information and the third entity comprises a navigation system.

1

ABSTRACT

2 A system and method for mass distribution of data products, such as geographic
3 databases. An authorization server maintains a first portion of each of several data products, and
4 each of several data distribution terminals maintains the second portion of each data product. A
5 user may couple a portable data storage device with a data distribution terminal and select a
6 desired data product. The terminal may then responsively obtain from the authorization server
7 the first portion of the selected data product and record onto the data storage device both the first
8 portion and second portion of the data product. The user may then couple the data storage device
9 with a machine, such as a navigation system, which may then access the data product. The
10 authorization server may secure the first portion before sending it to the data distribution
11 terminal. The authorization server may do so by encrypting the first portion and tying the first
12 portion together with an authorization key. The machine may then use the authorization key to
13 validate and/or facilitate access to the first portion and in turn to the data product as a whole.

14

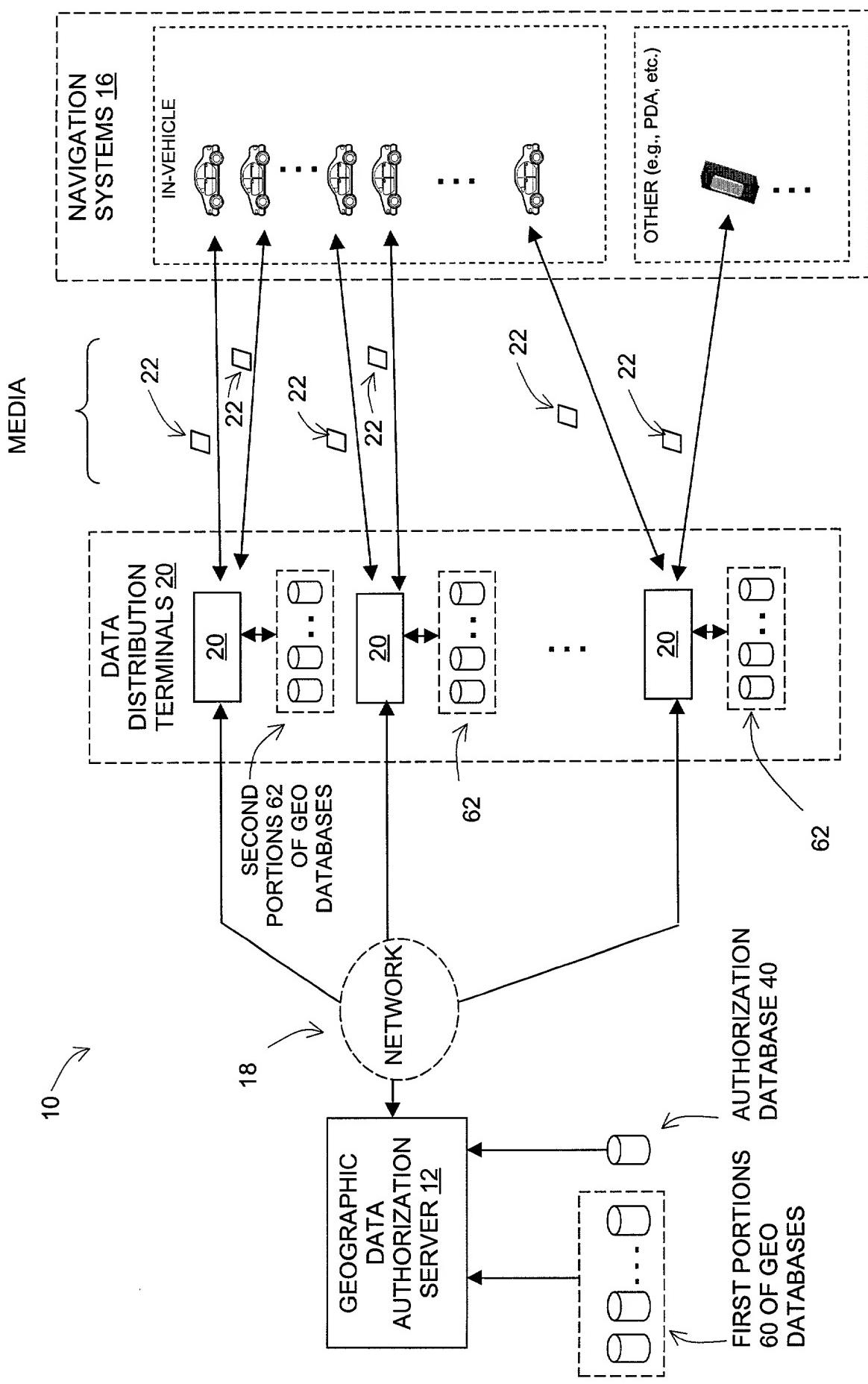


FIG. 1

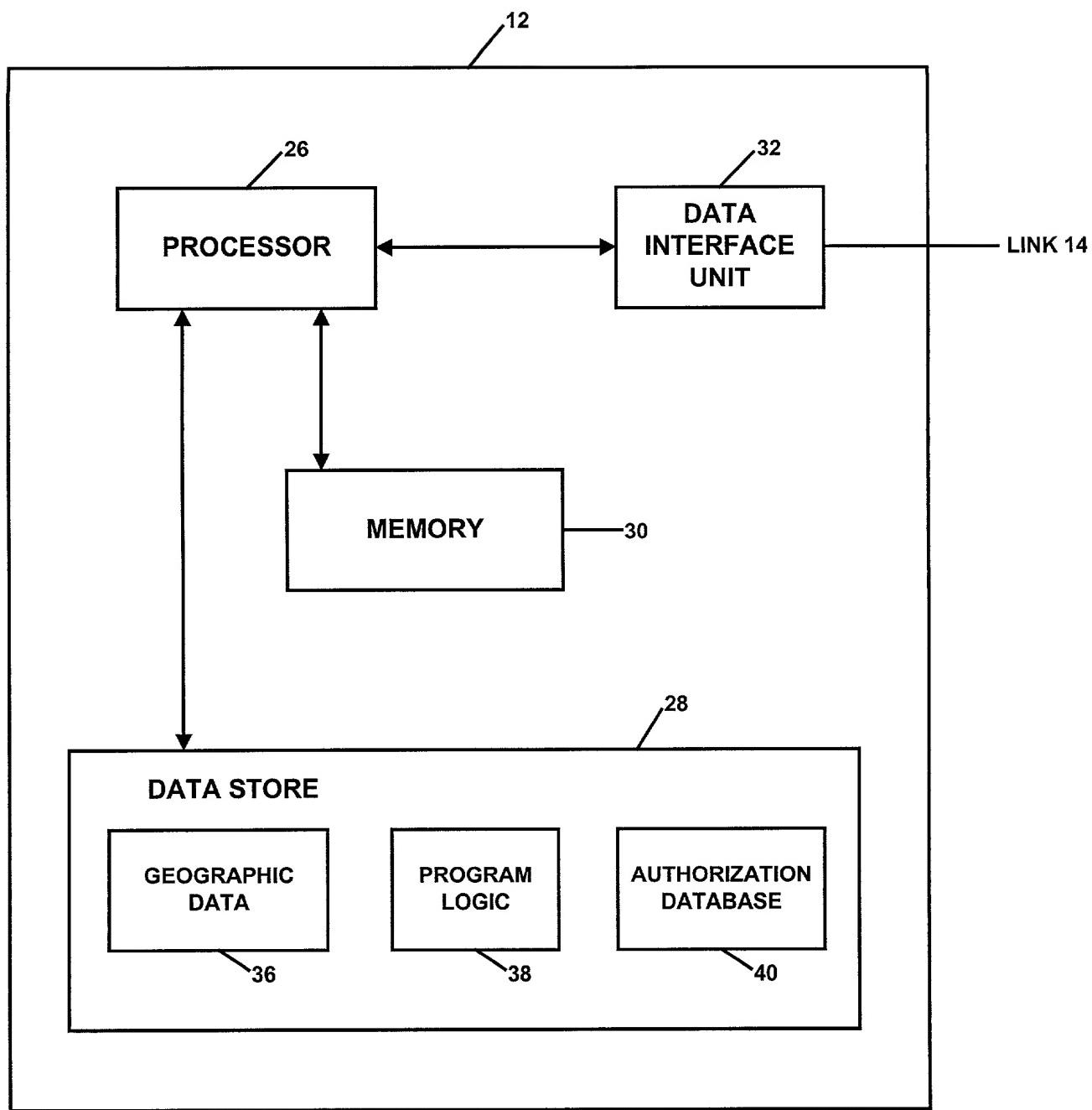


Fig. 2

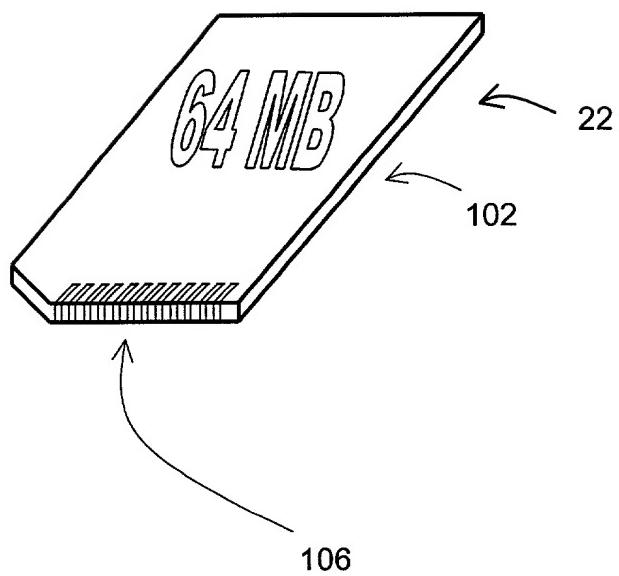


FIG. 3

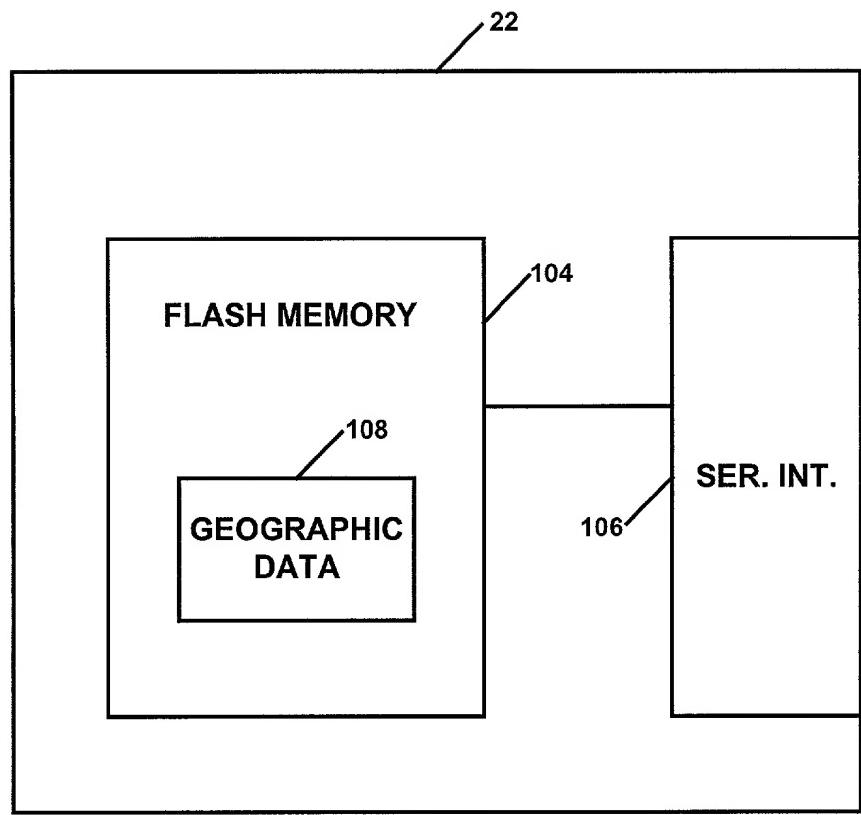


Fig. 4

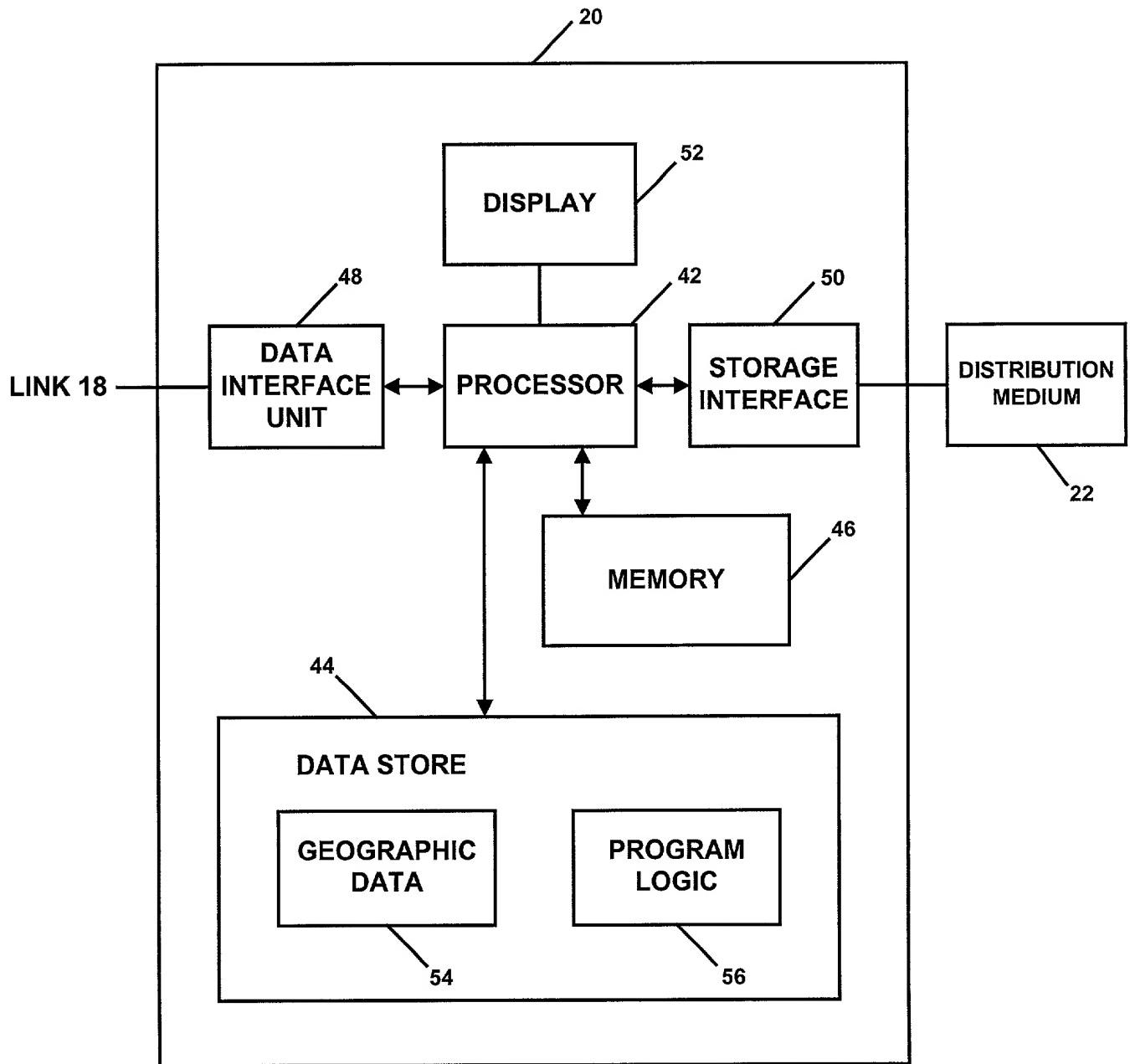
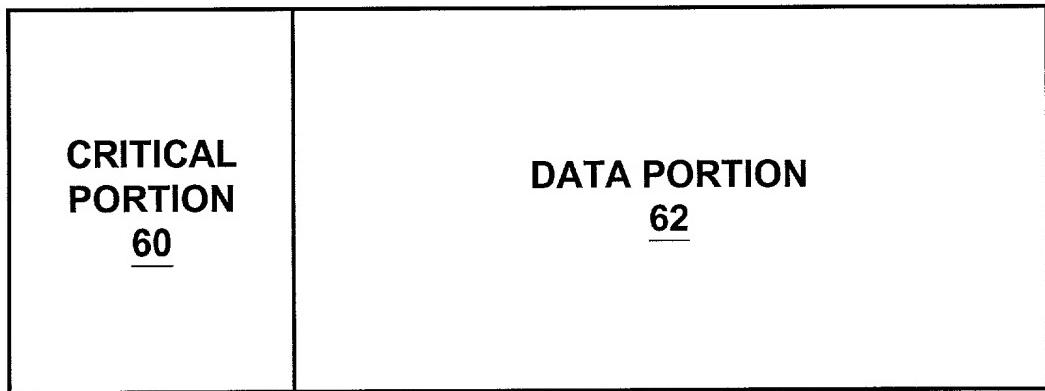


Fig. 5



58

A single black arrow originates from the number "58" and points towards the left edge of the large rectangular frame.

Fig. 6

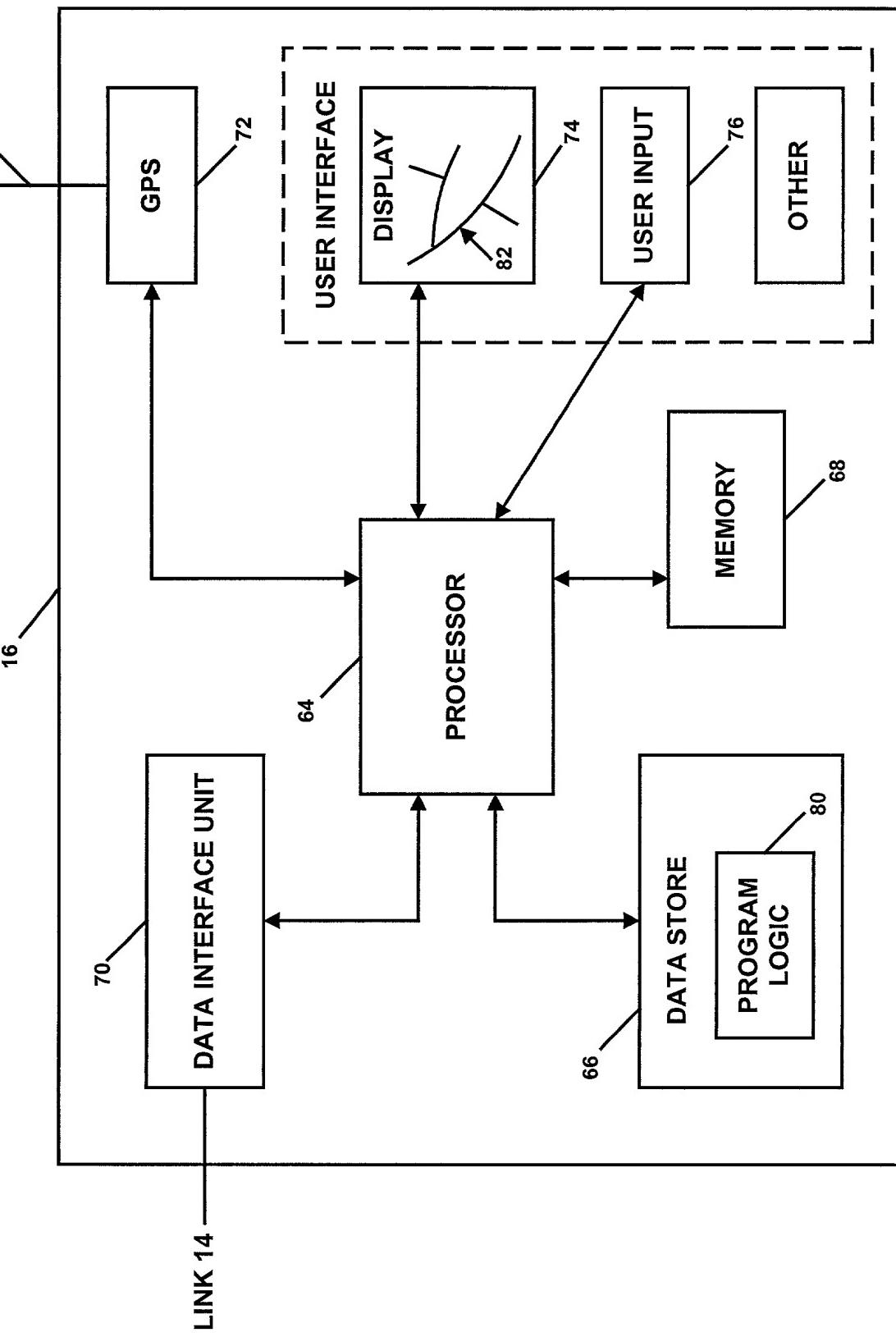


Fig. 7

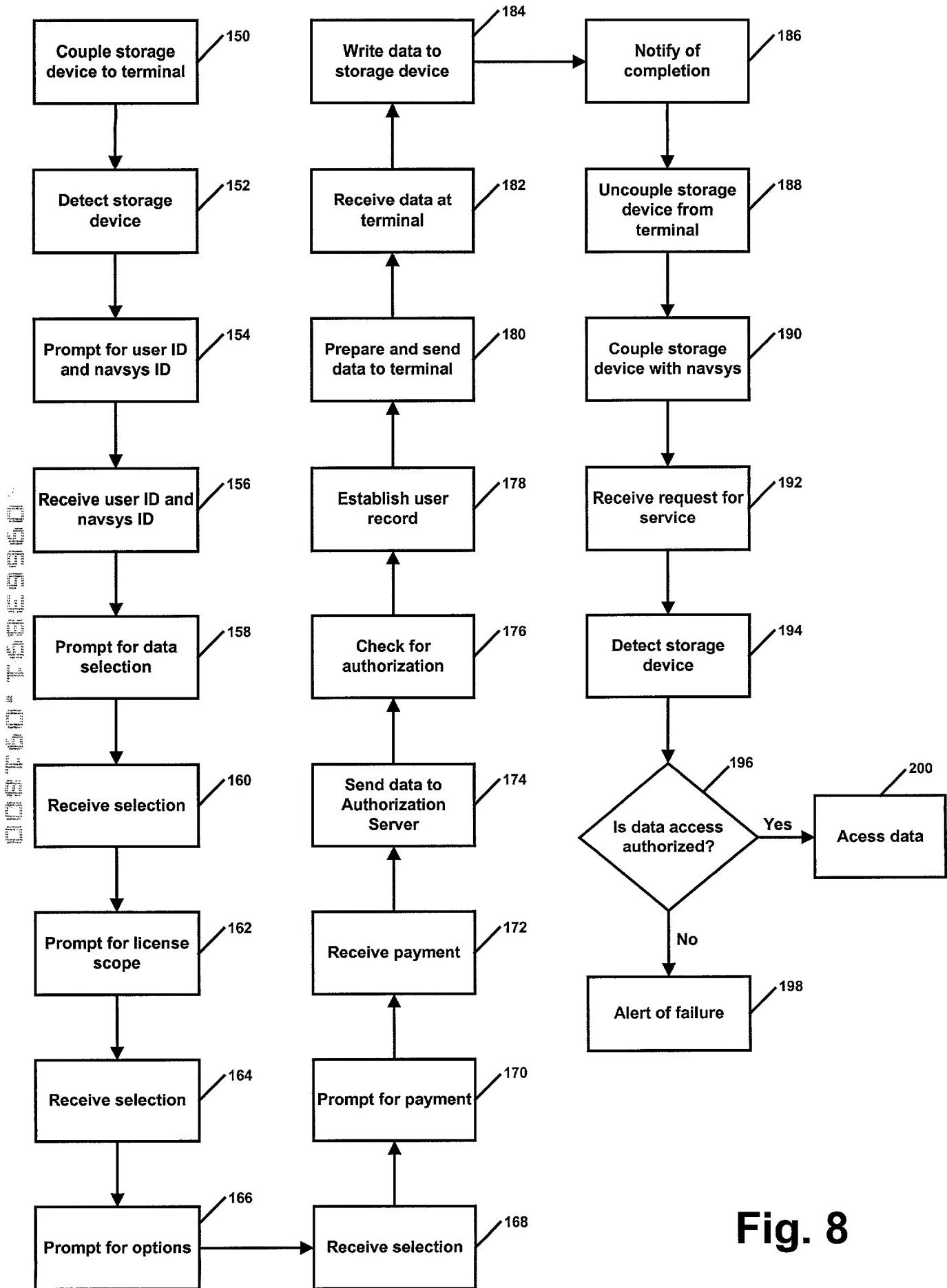


Fig. 8

Fig. 9

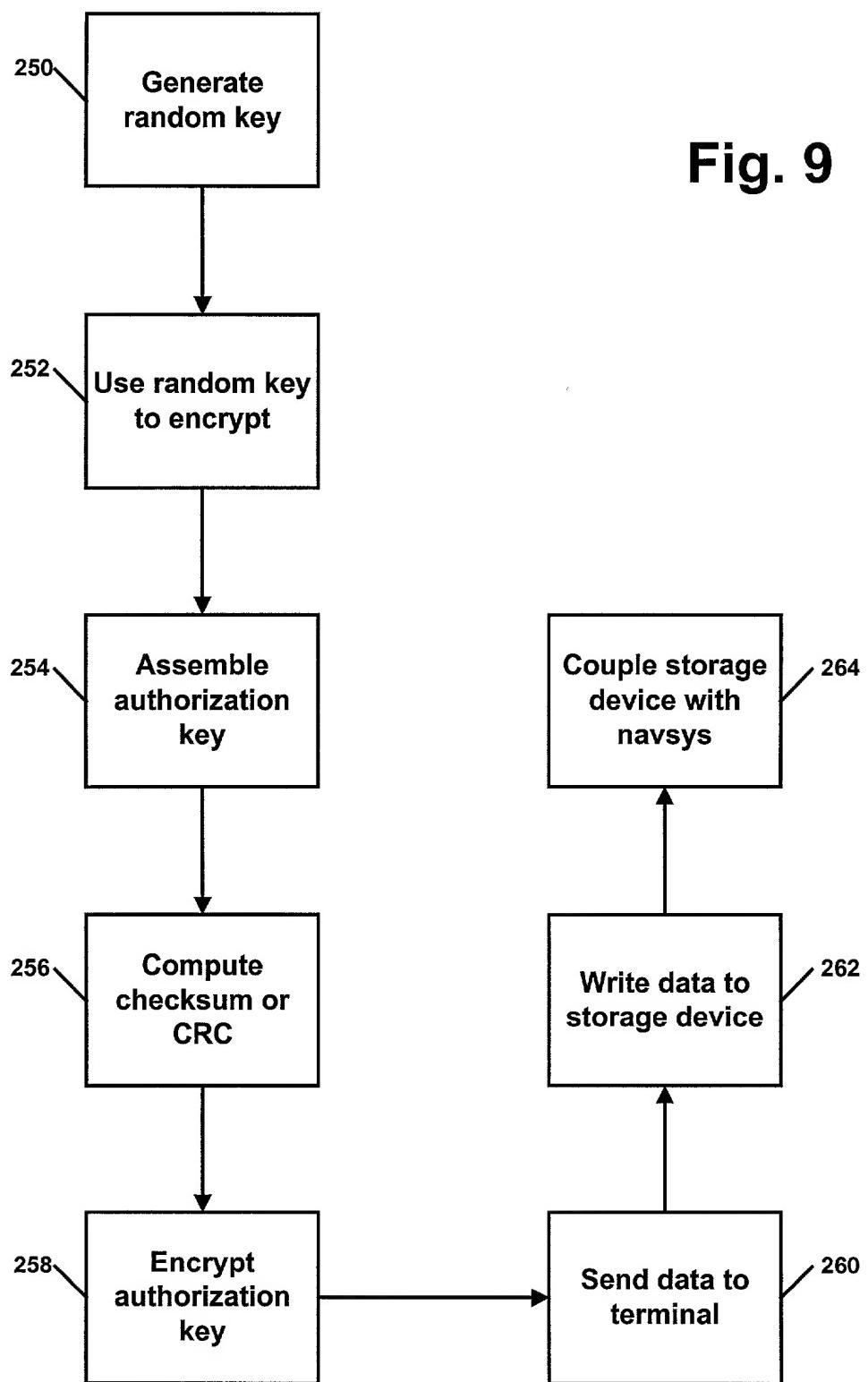


Fig. 10

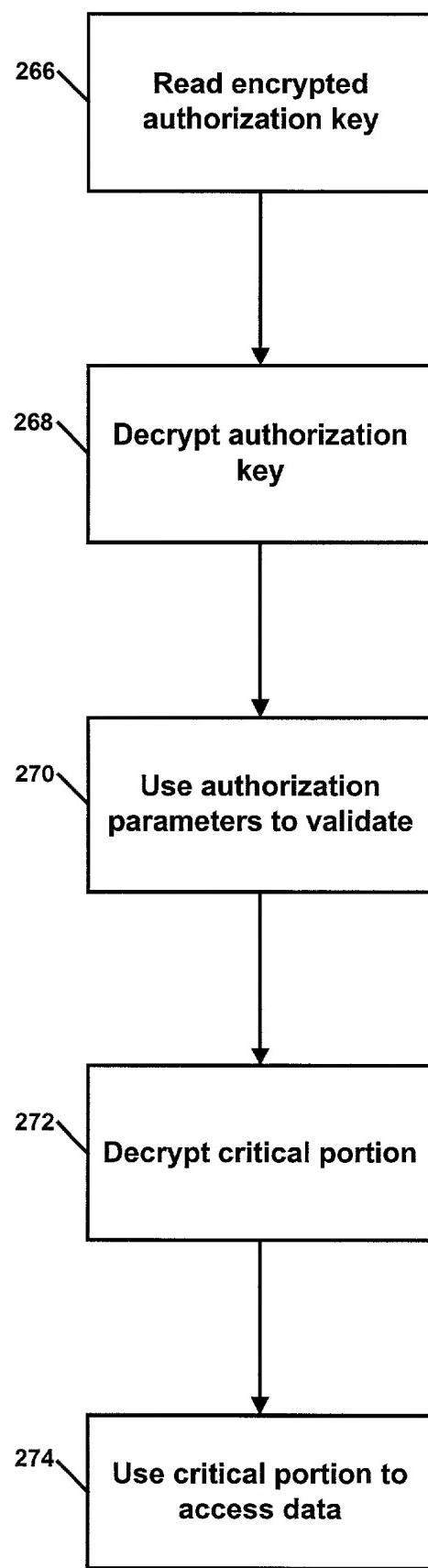
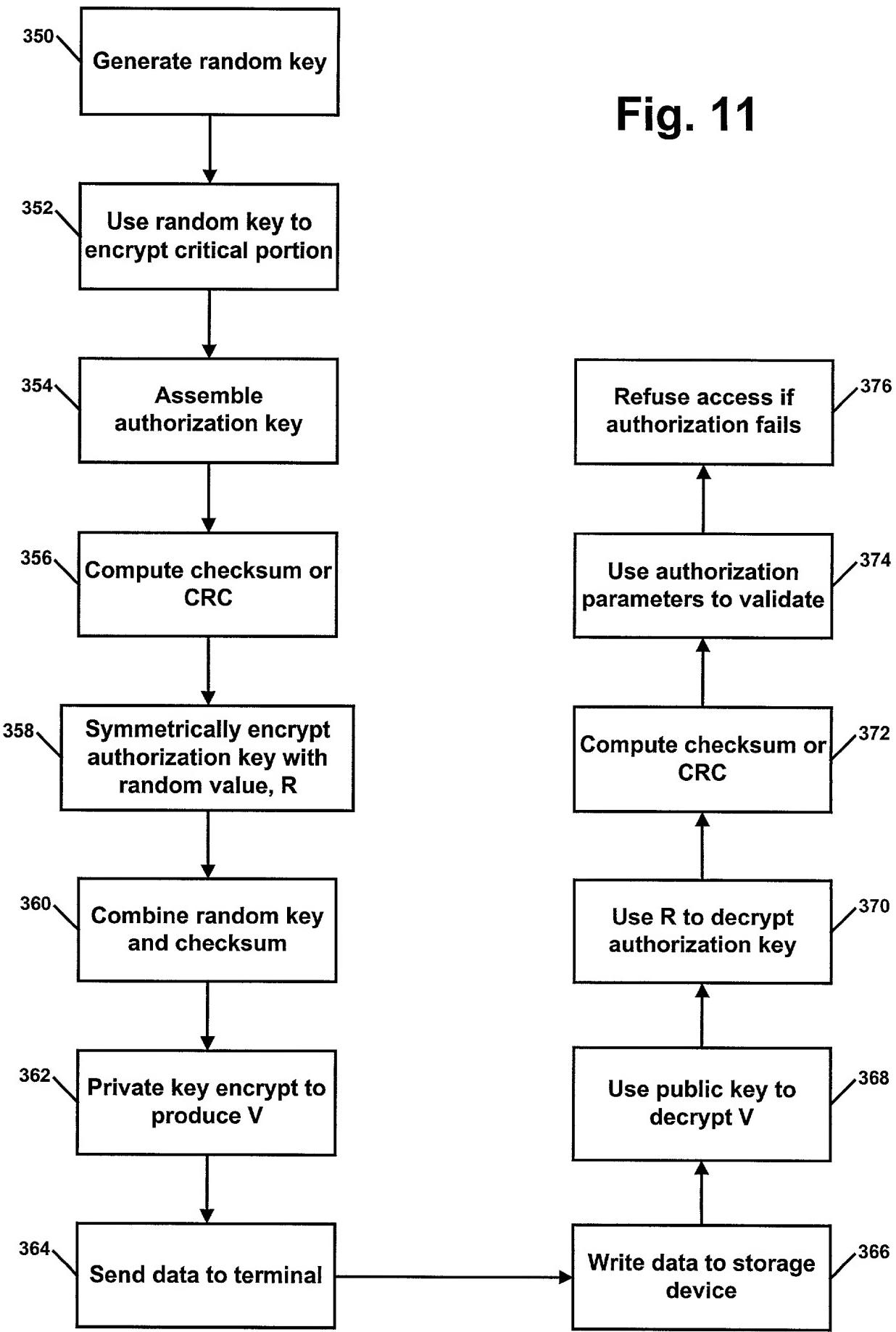


Fig. 11



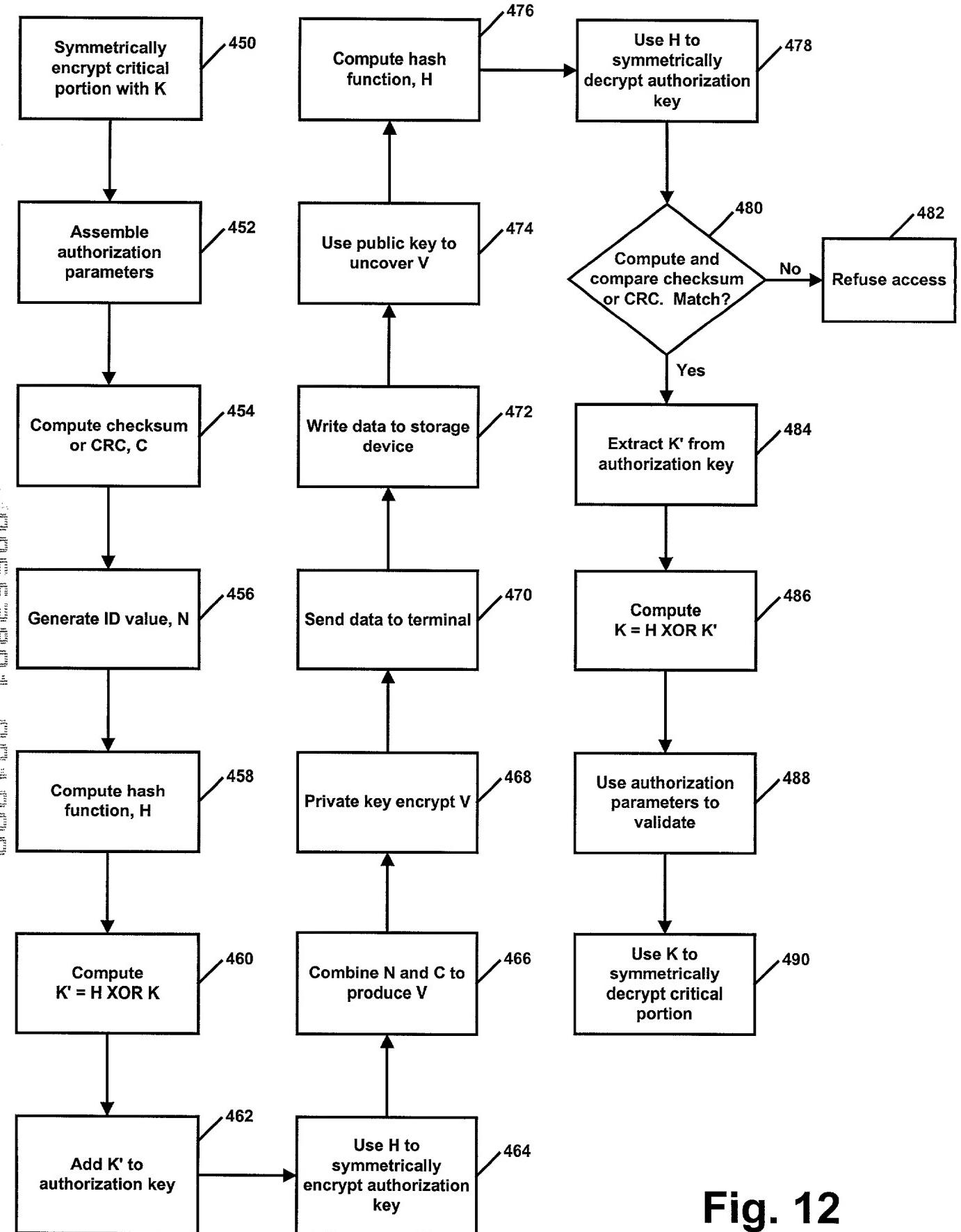
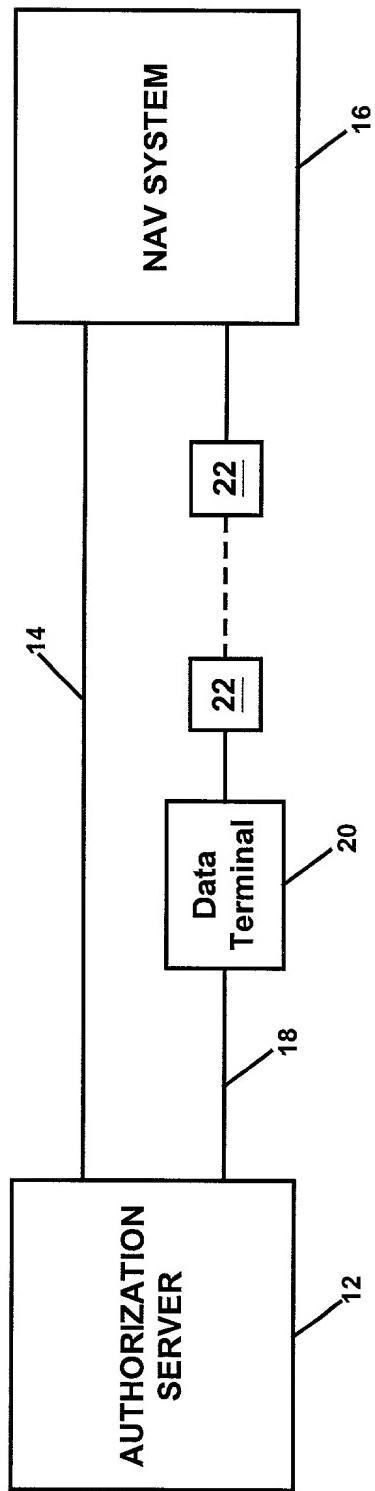


Fig. 12

Fig. 13



DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled, METHOD AND SYSTEM FOR MASS DISTRIBUTION OF GEOGRAPHIC DATA FOR NAVIGATION SYSTEMS, the specification of which:

- is attached hereto.
- was filed on _____ as Application Serial No. _____.
- and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability as defined in Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed:

<u>Prior Foreign Application(s)</u>			<u>Priority Claimed</u>
(Number)	(Country)	(Day/Month/Year Filed)	Yes <input type="checkbox"/> No <input type="checkbox"/>

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below:

(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)	(Filing Date)	None (Status-patented, pending, abandoned)

As a named inventor, I hereby appoint the following registered practitioners to prosecute said patent application and to transact all business in the Patent and Trademark Office connected therewith:

Frank J. Kozak (Reg. No. 32,908)
Lawrence M. Kaplan (Reg. No. 33,521)

Direct all correspondence for the above-identified application and telephone calls to:

FRANK J. KOZAK
Chief Patent Counsel
Navigation Technologies Corporation
10400 West Higgins Road
Rosemont, Illinois 60018
voice: (847) 795-7000 x7371
fax: (847) 795-7228

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor's Signature


Date: 18 Sept 2001

Full name of sole or first inventor

ROBERT CHOJNACKI

Residence

Chicago, Illinois

Citizenship

USA

Post Office Address

3909 North Kostner Avenue, Chicago, Illinois

60641

rev. Feb. 1999

U.S. PATENT AND TRADEMARK OFFICE